CA Service Desk Manager

Guida all'amministrazione

Versione 12.9.00

Riferimenti ai prodotti CA Technologies

Il presente documento fa riferimento ai seguenti prodotti CA Technologies:

- CA Asset Portfolio Management (CA APM)
- CA CMDB
- CA Business Intelligence
- CA Business Service Insight (CA BSI)
- CA Configuration Automation (precedentemente noto come CA Cohesion ACM)
- CA Embedded Entitlements Manager (CA EEM)
- CA Enterprise Workload Automation (CA EWA)
- CA Process Automation (precedentemente noto come CA IT PAM)
- Database di gestione CA (MDB)
- CA Management Portal
- CA Unicenter NSM (Network and Systems Management)
- Portale CA
- CA Remote Control Manager (CA RCM)
- CA Service Desk Manager (CA SDM)
- CA Service Management
- CA Siteminder
- CA Software Delivery
- CA Spectrum® Infrastructure Manager (CA Spectrum)
- CA Wily
- CA Workflow

Contattare il servizio di Supporto tecnico

Per l'assistenza tecnica in linea e un elenco completo delle sedi, degli orari del servizio di assistenza e dei numeri di telefono, contattare il Supporto tecnico visitando il sito Web all'indirizzo http://www.ca.com/worldwide.

Sommario

Capitolo 1: Introduzione 25

Destinatari 25
Informazioni necessarie 25
Processi e procedure ottimali per la gestione dei servizi 26

Capitolo 2: Gestione dei server 27

Numero di server 27
Modalità di modifica di una configurazione server 28
Modalità di avvio dei server di CA SDM 28
    Avvio dei server di CA SDM con la configurazione convenzionale 30
    Avviare i server di CA SDM con la configurazione di disponibilità avanzata. 31
Esecuzione della manutenzione progressiva sui server di CA SDM 32
    Verifica delle considerazioni 34
    Eliminazione del controllo versioni tra il server di standby e il server in background 35
    Promozione del server di standby come nuovo server in background 35
    Esecuzione della manutenzione progressiva sui server applicazioni 36
Modalità di configurazione dell'autenticazione SSL 38
    Verifica dei prerequisiti 39
    Impostazione della funzionalità del motore Web mediante i parametri Web Director 39
    Scegliere l'ambiente di accesso SSL 40
    Configurazione dell'ambiente di accesso SSL 42
Modalità di configurazione di TCP/IP 48
Modalità di distribuzione dei servizi Web CMDBf 49
Modalità di riavvio dei server CA SDM 49
    Riavvio dei server di CA SDM con la configurazione convenzionale 49
    Riavviare i server di CA SDM con la configurazione di disponibilità avanzata. 49
Modalità di arresto dei server di CA SDM 52
    Arrestare i server di CA SDM con la configurazione convenzionale. 52
    Arrestare i server di CA SDM con la configurazione di disponibilità avanzata. 53
Supporto di tablet 56
Accesso a Tomcat 58
    Impostazioni predefinite del servlet 59
Interfaccia PDA 59
Registrazione REST 60
    Abilitazione della registrazione CXF 61
Configurazione dei processi per i server di CA SDM 67

Aggiunta di un server 68
Creazione della configurazione di un processo 69
Aggiunta dei processi al server di CA SDM 71
Verifica della configurazione 84

Capitolo 3: Interfaccia utente mobile REST di esempio 85

Modalità di distribuzione dell'interfaccia utente mobile di esempio REST 87
Configurazione dei servizi Web REST 88
Abilitazione dell'interfaccia utente mobile REST di esempio 89
Gestione degli incidenti dall'interfaccia mobile REST di esempio 89
Esempio: Pagina iniziale dell'interfaccia Analista 90
Esempio: Pagina iniziale dell'interfaccia Dipendente 91
Esempio: Creazione di un Incidente da parte di un dipendente 92

Capitolo 4: Configurazione di CA SDM Mobile Enabler 93

CA SDM Mobile Enabler 93
Coda analista 94
Approvazioni 95
Open Space 98
Verifica dei prerequisiti 99
Sistemi operativi mobili certificati 99
Applicazione delle patch per Open Space 100
Abilitazione delle impostazioni CORS 100
(Facoltativo) Impostazione dei campi del modulo come non obbligatori 102
(Facoltativo) Applicazione della compatibilità delle approvazioni dopo l'aggiornamento 103
Accedere a CA SDM Mobile Enabler 103

Capitolo 5: Definizione della struttura del business 105

Creazione della struttura aziendale 106
Modalità di creazione della struttura aziendale 109
Definizione dell'infrastruttura aziendale 119
Ordine di definizione degli oggetti 120
Famiglie e classi 120
Produttori e modelli 120
Stato servizio 121
Tipi di fornitore e fornitori 121
Elementi di configurazione 121
Strumenti di gestione degli asset esterni 122
Multi-Tenancy 123
Fornitore servizio 123

Descrizione della funzione multi-tenancy 124
Impatto sull'interfaccia utente 131
Impatto su Automazione supporto 134
Impatto su Gestione della conoscenza 135
Modalità di utilizzo di multi-tenancy 136

Capitolo 6: Integrazione di più motori di ricerca mediante la ricerca federata 147

Configurazione della ricerca federata 148
Completamento dei prerequisiti 149
Abilitazione della ricerca federata 150
Generazione dei file XML di configurazione per la ricerca federata 150
Creazione delle origini di ricerca federata in CA SDM 157
Disinstallazione dell'adapter di ricerca 158
Configurazione della superficie crawler 159
Completamento dei prerequisiti 160
Creazione della superficie crawler dell'utente di CA SDM 160
Configurazione del filtro indirizzi IP remoti di Tomcat 161
Configurazione dell'ID utente della superficie crawler 163
Configurazione del crawler SharePoint 170
Creazione dell'origine di contenuto in SharePoint 171
Creazione delle regole di ricerca per indicizzazione 172
Avvio di ricerca per indicizzazione in SharePoint 173
Configurazione dei metadati in SharePoint 174
Verifica dei dati crawler in SharePoint 175
Risoluzione dei problemi 176
Creazione di un nuovo adapter personalizzato mediante l'interfaccia SDK 178
Compilazione dei file JAR per il nuovo adapter personalizzato 180
Configurazione del nuovo adapter di ricerca personalizzato con il componente CAFedSearch 183
Verifica del nuovo adapter di ricerca personalizzato 185
Aggiunta di un filtro CORS 186
Chiamata del servlet CAFedSearch tramite REST 187

Capitolo 7: Implementazione delle policy 189

Implementazione dei criteri 189
Notifiche 189
Integrazione di CA SDM 298

Capitolo 8: Configurazione degli account utente 319

Contatti 319

Definizioni dei contatti 319
Gruppi 321
Tipi contatto 322
Comportamento in base al tipo di contatto 322
Configurazione della notifica in base al tipo di contatto 322
Selezione dei contatti in base al tipo di contatto 322
Tipi di gestione speciali 323
Modalità di configurazione di contatti di gestione speciale 324
Associazione di un contatto con un tipo di gestione speciale 325
Dati di directory LDAP 326

Capitolo 9: Gestione dei ruoli 351

Ruoli 351
Ruoli predefiniti 351
Protezione Role-Based 353
Modalità di funzionamento dei tipi di accesso 354
Record ruolo 357
Aree di accesso funzionale 358
Partizioni dati 363
Navigazione basata su ruoli 363
Schede 364
Schede predefinite 365
Moduli Web 367
Gruppi moduli 368
Strutture menu 368
Risorse struttura menu 369
Barre dei menu 370
Barre degli strumenti 371
Risorse di accesso rapido 371
Set di file della Guida 372
Modalità di implementazione di un ruolo personalizzato 372
Modalità di implementazione di una struttura menu personalizzata 374
Creazione di un record ruolo 375
Creazione di un record scheda 376
Creazione di un record barra dei menu 377
Creazione di record di modulo Web 378
Copia di una struttura menu 379
Creazione e personalizzazione di una struttura menu 380
Creazione e pubblicazione di un set di file della Guida 381
Cambio dei ruoli 383

Capitolo 10: Definizione della struttura di supporto 385

Modelli ...385
- Modello interno ...386
- Modello esterno ...387
- Modello combinato ...388

CA Workflow ...389
- Flusso di lavoro in runtime ...390
- Selezione di una definizione di processo CA Workflow ...390
- Attività flusso di lavoro ...391

Integrazione del flusso di lavoro di CA Process Automation ...392
- Componenti di CA Process Automation ...393
- Integrazione di CA Process Automation con CA SDM all'esecuzione ...393
- Modalità di creazione di una definizione di processo ...394
- Creazione di un modulo richiesta di avvio ...395
- Associazione di una definizione di processo di CA Process Automation ...397

Codici condivisi ...398
- Codici di priorità ...399
- Codici di gravità ...400
- Codici di impatto ...400
- Codici di urgenza ...400

Codici stato ...401
- Codici stato richiesta ...401
- Codici stato ordine di cambiamento ...403
- Codici stato questione ...404
- Codici stato attività ...405

Tipi di attività ...406
- Installazione del tracciamento degli incidenti ...407

Aree Richiesta/Incidente/Problema ...408
- Proprietà area richiesta/incidente/problema ...409
- Definizione di aree richiesta/incidente/problema per l'interfaccia self-service ...411

Categorie Ordine di cambiamento e Issue ...411
- Categorie di cambiamento predefinite ...412
- Categorie di questione predefinite ...413
- Regole per la modifica delle categorie in un ticket ...413
- Proprietà delle categorie ...414
- Definizione di categorie questione e cambiamento per l'interfaccia self-service ...416

Chiusura automatica dei ticket ...417
- Modalità di definizione delle impostazioni di chiusura automatica dei ticket ...417
- Modalità di definizione di una notifica di attività di chiusura automatica ...418

Attività correlate ai ticket ...419
- Modalità di definizione di attività di notifica per ticket correlati ...420

Modalità di definizione delle notifiche attività ticket correlati ... 420
Calcolo della priorità ... 421
Modalità di gestione dei valori dei ticket da parte del calcolo della priorità ... 423
Generazione del valore di urgenza dopo il salvataggio del ticket mediante il calcolo della priorità ... 425
Modalità di impostazione del calcolo della priorità ... 427
Controlli di attributo dipendenti e transizioni di stato ... 437
Modalità di lavoro con controlli di attributo dipendenti e transizioni di stato ... 438
Configurazione di transizioni di stato ... 439
Configurazione di controlli di attributo dipendenti ... 440
Metodi dei servizi Web ... 441
Flussi di transizioni predefiniti ... 442
Procedura ottimale: Transizioni di stato predefinite ... 446
Transizioni di stato per l'interfaccia self-service ... 448
Modalità di funzionamento delle transizioni per l'interfaccia self-service ... 448
Modalità di creazione o aggiornamento di tipi di transizione per le transizioni ... 449
Modalità di collegamento dei tipi di transizione alle transizioni ... 450
Attivazione dei tipi di transizione predefiniti ... 450
Timer ... 452
Fusi orari ... 453
Attivazione di eventi tipo di servizio ... 453
Evento attivato dal fuso orario ... 454
Regole fuso orario ... 454
Modalità di configurazione della libreria allegati ... 455
Apertura dell'interfaccia utente Web di CA SDM ... 456
Creazione di un tipo di file ... 457
Scelta del repository ... 458
Creazione di una cartella ... 464
Annunci ... 465
Visibilità degli annunci interni ... 466
Definizione dell'urgenza degli annunci ... 467
Configurazione delle query memorizzate ... 467
Numeri di sequenza ... 468
Uso del registro di audit ... 469
Integrazione con CA Network and Systems Management ... 470
Stampa di pagine Web CA SDM ... 470
Blocco dei record nell'interfaccia Web ... 471
Struttura di supporto ... 471
Abilitazione della Guida in linea di CAPA ... 472

Capitolo 11: Controllo del comportamento del sistema 475

Utilizzo di Gestione opzioni ... 475

Modalità di modifica dell'ambiente di sistema ... 476

Capitolo 12: Configurazione dell'assegnazione automatica 483

Assegnazione automatica ... 483
Relazioni di assegnazione automatica ... 484
Metodi di assegnazione automatica ... 484
Modalità di avvio dell'implementazione dell'assegnazione automatica ... 485
Aree e categorie ... 485
Gruppi di analisti ... 486
Analisti ... 486
Assegnazione automatica di ticket a un gruppo e non ai contatti presenti nel gruppo ... 487
Assegnazione automatica in base alla posizione ... 488
Assegnazione automatica in base ai turni ... 489
Gruppo e assegnatario predefiniti ... 491
Abilitazione dell'assegnazione automatica ... 491
Sostituzione dell'assegnazione automatica ... 492
Controlli di assegnazione ... 493
Assegnazione manuale ... 493
Opzione Assignee_set ... 493
Iss assignee_set ... 494
Area_Defaults ... 494
Opzioni richiesta per assegnatari e gruppi ... 494
Modelli ... 495
Interfaccia di CA Network and Systems Management ... 496
Registro attività ... 496
Abilitazione della registrazione delle attività per gli attributi aggiuntivi ... 497
Tracciamento dell'assegnazione automatica ... 497
Query memorizzate ... 498
Modalità di assegnazione automatica dei ticket ... 498
Assegnazione automatica delle attività flusso di lavoro ... 505
Assegnazioni automatiche basate sull'elemento della configurazione ... 509
Modalità di funzionamento dell'assegnazione automatica basata su elementi della configurazione ... 509
Attivazione delle assegnazioni automatiche basate sull'elemento della configurazione ... 513

Capitolo 13: Gestione del database 515

Utilità di gestione del database ... 515
Selezione e configurazione del database ... 515
Utilità di caricamento del database ... 516
Modalità di creazione e utilizzo di un file di input ... 517
Eliminazione e ripristino dei vincoli ... 518
Backup del database ... 519

Ripristino del database 519
Sostituzione delle tabelle del database 519
Estrazione dei dati 520
Annullamento dei riferimenti dati 521
Esempio di utilizzo di pdm_deref 522
Uso della modalità dbadmin 524
Miglioramento delle prestazioni con la cache del browser 536
Configurazione di Microsoft Internet Information Server 536
Configurazione di Apache 537
Cancellazione della cache 538
Modifica del file di configurazione 538
SchedExpMaximum 547
SelListCacheExclude 548
SelListCacheMax 548

Capitolo 14: Utilizzo dell'API testo 553

API testo 553
Interfaccia della riga di comando 554
Interfaccia di CA Network and Systems Management 554
Formato input 555
Parole chiave 556
Convenzioni di immissione delle parole chiave 558
Formattazione di un messaggio di posta elettronica per aggiornare un ticket 559
Delimitatori di inizio e fine dei messaggi di posta elettronica 560
Modalità di utilizzo degli elementi da parte dell'interfaccia API testo 560
Modalità di impostazione di risposte a notifiche di posta per l'aggiornamento di ticket 561
Metodi di conversione 565
File di configurazione 567

Capitolo 15: Controllo delle versioni per le personalizzazioni di sistema nei vari server di CA SDM 571

Verifica dei prerequisiti 572
Modifica del file di controllo versioni del server 573
Componenti di controllo versioni 574
Parametri del servizio Controllo versione 575
Riavvio di CA SDM sul client 579
Scegliere il server applicazioni meno attivo 579
Arresto dell'altro server applicazioni 580
Verifica delle personalizzazioni sul client 580

Capitolo 16: Gestione degli elementi di configurazione 583

Utilizzo dell'interfaccia Web 583
Visualizzazione degli elementi della configurazione 584
Creazione di un elemento della configurazione 585
Aggiornamento di un elemento della configurazione 585
Associazione di una finestra di manutenzione con un elemento della configurazione 586
Visualizzazione di finestre di cambiamento associate 587
Visualizzazione della cronologia degli elementi di configurazione 587
Disattivazione di un elemento di configurazione 587
Riattivazione di un elemento di configurazione 588
Contatto, posizione ed elementi della configurazione dell'organizzazione 588
Creazione di un elemento della configurazione da un oggetto base 589
Selezione di un oggetto di base per un elemento di configurazione 590
Modifica dei dettagli relativi a un elemento della configurazione per un oggetto di base 590
Modifica degli attributi degli elementi della configurazione per un oggetto base 591
Creazione di un elemento di configurazione per un oggetto di base utilizzando GRLoader 592
Relazioni elemento della configurazione 592
Tipi relazioni elementi della conoscenza 593
Creazione di un tipo di relazione 594
Gestione della relazione degli elementi della configurazione 595
Creazione di una relazione degli elementi della configurazione 595
Visualizzazione delle relazioni per un elemento di configurazione 596
Disattivazione di una relazione di un elemento della configurazione 596
Riattivazione di una relazione degli elementi della configurazione 597
Disattivazione di relazioni di elementi della configurazione (Modifica in elenco) 597
Disattivazione di una relazione dell'elemento della configurazione utilizzando GRLoader 598
Riattivazione di una relazione dell'elemento della configurazione utilizzando GRLoader 599
Eliminazione di una relazione di elementi della configurazione dal database 600
Cronologia e confronto di una relazione di elemento della configurazione 600
Controllo delle versioni 601
Utilizzo del controllo delle versioni 603
Record di audit trail per asset ed elementi della configurazione condivisi 604
Terminologia relativa al controllo delle versioni 605
Origini dei dati di controllo delle versioni 608
Integrazione della gestione della modifica SDM degli elementi della configurazione 609
CA APM Integrazione 610
Gestione del controllo delle versioni degli elementi della configurazione 611
Gestione delle modifiche in CA SDM 632
Visualizzazione degli attributi degli elementi della configurazione in altri prodotti CA 633
Utilizzo di Visualizzatore CMDBf 634
Visualizzatore CMDB 634

Analisi della causa principale 637
Amministrazione del visualizzatore 637
Aggiunta di un asset rilevato 638
Flag di asset ed elementi della configurazione 639
Riconciliazione elementi della configurazione 640
Riconciliazione basata su MDR....641
Identificazione e risoluzione degli elementi della configurazione ambigui 643
Revisione e modifica di dati in entrata utilizzando l'area di lavoro della transazione (TWA) 657
Gestione di transazioni con installazione di appoggio 663
Area di lavoro transazione 664
Compilazione dell'area di lavoro transazione (TWA) 666
Modalità di utilizzo dell'interfaccia Web per aggiornare i dati nell'area di lavoro transazione (TWA)....678
Gestione di transazioni di relazione 681
Modalità di caricamento delle transazioni in CMDB....682
Amministrazione dell'area di lavoro transazione (TWA)....684
Manutenzione dei dati di CA CMDB 688
Struttura delle classi/famiglie di CA CMDB 689
Modifica della famiglia/classe di un singolo elemento della configurazione....690
Modifica della famiglia/classe di un elenco di elementi della configurazione....690
Modifica della famiglia/classe di elementi della configurazione con GRLoader 691
Estensione di CA CMDB....691
Funzionalità CACF (Configuration Audit and Control Facility)....703
Amministrazione della funzionalità CACF e definizione delle policy....705
Attributi gestiti 721
Stati del Cambiamento gestito....722
Specifiche del Cambiamento....724
Modalità di funzionamento della verifica del Cambiamento....730
Archiviazione ed eliminazione dei dati di audit 736
Implementazione della strategia di verifica del Cambiamento. 737
Progettazione e implementazione della verifica di Cambiamento. 742
Procedure consigliate di verifica dei Cambiamenti....749
Verifica manuale di aggiornamento del valore dell'attributo dell'elemento della configurazione 753
Esempio: Autorizzazione degli aggiornamenti non autorizzati solo da una posizione specifica....758
Esempio: Aggiornamento dei computer portatili dell'organizzazione....760
Esempio: Blocco degli Ordini di cambiamento non verificati 761
Esempio: Autorizzazione dell'aggiornamento dell'elemento della configurazione nel caso in cui non esista un Ordine di cambiamento corrispondente 762
Esempio: Rinvio degli aggiornamenti da CA Configuration Automation all'area di lavoro della transazione....762
Esempio: Registrazione dei risultati della policy come test 763
Esempio: Rifiuto dell'aggiornamento di un elemento della configurazione 763
Esempio: Autorizzazione di Ordini di cambiamento creati senza specifiche 764

Esempio: Blocco dell'autorizzazione di Ordini di cambiamento creati senza specifiche 764
Esempio: Autorizzazione degli inserimenti non autorizzati da origini selezionate 765
Esempio: Autorizzazione di un aggiornamento non autorizzato per un elemento della configurazione non appartenente alla produzione 765

Capitolo 17: Amministrazione degli MDR 767

Informazioni su MDR....767
Classi MDR e nomi MDR....768
Come avviene l'integrazione di un MDR con CA SDM?....768
Definizione di un MDR su CA SDM 769
Utilità di avvio MDR....769
Definizione di un URL per avviare un MDR 770
Impostazione di un fornitore MDR CA APM....772
Avvio diretto nel contesto da CA CMDB a CA APM 772
Proprietà dell'elemento condiviso che supportano la federazione MDR. 773
ID asset federato 773
Nome MDR....774
Classe MDR....774
Definizione MDR con l'installazione di CA Cohesion ACM 774
MDR CA Cohesion ACM....775
Modalità di associazione manuale di un MDR a un elemento della configurazione 776
Importazione automatica da CA Cohesion....777
Mapping di un elemento della configurazione a un MDR....777
Amministrazione delle definizioni MDR....778
Report di CA Cohesion ACM....779
Utilizzo di GRLoader 779
Convenzioni di denominazione per gli elementi della configurazione e limitazioni 780
Convenzione di denominazione per nome_sistema 781
Utilizzo di Visualizzatore CMDBf 782
Modalità di aggiornamento di file di metadati per la mappatura CMDBf 783
Modalità di visualizzazione di valori di attributo MDR con nomi di attributo CA CMDB 784
Come nascondere attributi di fornitore MDR 785
Definizione degli attributi MDR senza equivalenti CA CMDB 786
Definizione di metadati del fornitore di dati CMDBf 786

Capitolo 18: Gestione delle modifiche 787

Gestione Cambiamento di CA SDM....787
Componenti di Gestione cambiamento 788
Visualizzazione del calendario dei Cambiamenti 789
Responsabilità del gruppo CAB 790
Modalità di funzionamento del processo CAB....791

Assegnazione dei membri al gruppo CAB 791
Responsabilità di Gestione cambiamenti 792
Funzionamento del ruolo Gestione cambiamenti 793
Definizione delle attività per il ruolo Gestione cambiamenti 793
Categorie di cambiamento, stato e livelli di rischio 794
Visualizzazione del contatore degli ordini di cambiamento 795
Definizione di una query memorizzata per ordini di cambiamento 796
Configurazione delle opzioni di Gestione cambiamenti 797
Calendario dei Cambiamenti 798
Aggiunta delle informazioni di pianificazione ad un ordine di cambiamento 798
Modelli eventi iCalendar 799
Esportazione delle pianificazioni in iCalendar 800
Visualizzazioni di pianificazione 801
Configurazione della visualizzazione di pianificazione 803
Modalità di pianificazione degli Ordini di cambiamento 811
Esempio di utilizzo dell'utilità di pianificazione dei cambiamenti 812
Modalità di pianificazione delle finestre di cambiamento 816
Visualizzazione di finestre di cambiamento 817
Associazione di un elemento della configurazione con una finestra di manutenzione 818
Visualizzazione di elementi della configurazione associati 818
Esempio di creazione di una finestra di blackout 819
Creazione di una finestra di manutenzione globale 820
Analisi e rilevamento dei conflitti 820
Visualizzazione di CA Workflow 821
Modalità di visualizzazione del flusso di lavoro 821
Definizione del processo Gestione Cambiamento per CA Workflow 823
Componenti della definizione di processo della Gestione cambiamento 824
Come configurare la definizione dei processi di gestione dei cambiamenti 824
Funzionamento della definizione del processo Gestione Cambiamento 831
Attore ActivityNode non trovato: Aggiorna oggetto -Service Desk r12 845
L'ordine di cambiamento non si chiude 846
Console CAB e reporting 846
Gestione dei gruppi CAB 847
Assegnazione dei gruppi CAB 849
Approvazioni CAB 849
Cambiamento delle proprietà della console CAB 849
Funzionalità di reporting del ruolo Gestione cambiamento 851
Valutazione dei rischi 852
Modalità di implementazione di un'indagine di rischio 852
Modalità di accesso a un'indagine di rischio direttamente da un URL 854
Impact Explorer 855
Avvio di Impact Explorer 856

Esplorazione degli elementi della configurazione associati. 856
Visualizzazione di un elemento della configurazione in Impact Explorer 857
Aggiunta di un elemento della configurazione correlato a un ordine di cambiamento 857
Visualizzazione dell'elenco di elementi della configurazione figlio 858
Avvio di CMDB Visualizer da Impact Explorer 858
Configurazione di Impact Explorer 859

Capitolo 19: Gestione dei rapporti 861

Capitolo 20: Report CA Business Intelligence 863

Scenari di reporting 863
Componenti del reporting 864
Diagramma di flusso sul reporting dei dati 866
Visualizzazione dei report Web in InfoView 867
Protezione e autorizzazione 868
Gruppi e utenti 868
Partizioni di dati CA SDM in Infoview 869
Universo e collegamenti dell'universo 869
Cartelle di report 870
Livelli di accesso 872
Modalità di indirizzamento di un server di CA Business Intelligence esistente a un server CA SDM 873
Creazione di una fonte dati ODBC. 873
Configurazione dell'universo 874
Esportazione dell'universo 875
Modalità di configurazione della protezione delle partizioni dati per il reporting 875
Aggiungere l'utente privilegiato CA SDM a CMC 876
Definizione di credenziali del database universo 876
Definizione delle partizioni dati 877
Database replicato per il reporting non in linea 878
Report Role-Based 878
Definizione dei report basati su ruoli per un ruolo 878
Visualizzazione dei nuovi report nella scheda Report 880
Report basati sul Web 887
Interfaccia di BusinessObjects InfoView 887
Spostamento tra i report 888
Preferenze di InfoView 888
Pianificazione dei report 888
Impostazione dell'analisi dei dati 889
Pubblicazione e distribuzione dei report 890
Indicatori di prestazioni chiave 890
Tipi di KPI 891

KPI predefiniti 891
Daemon KPI 891
KPIs sistema 892
KPI delle query memorizzate 894
KPI SQL 895
Campi KPI 896
Recupero dei dati del ticket 897
Risoluzione dei problemi 900
Report ad hoc 902
Interfaccia Web Intelligence 902
Funzionamento del reporting ad hoc 903
Esempio di report ad hoc 903
Esempio: visualizzazione di tutte le richieste con priorità aperta 1 e 2 per tutti gli utenti 904
Esempio: visualizzazione di tutte le richieste che non includono lo stato Work In Progress 905
Esempio: visualizzazione di tutte le richieste chiuse negli ultimi 30 giorni per gli utenti il cui cognome inizia con "C" 907
Report del dashboard 909
Visualizzazione di dashboard e report in InfoView 909
Scrivere report di CA Business Intelligence 910
Driver ODBC CA SDM 910
Stesura rapporti SQL per BusinessObjects 911
Funzioni PDM 912
Alias attributi 914
pdm_isql Interactive SQL 914

Capitolo 21: Creazione di report in CA SDM 915

Generazione rapporti 915
Visualizzazioni di database 915
Visualizzazioni di base 916
Visualizzazioni avanzate 918
Impostazione dei metodi di reporting 919
Formattazione dei report 919
Modifica del tipo di ordinamento delle colonne 920
Rapporti riepilogativi e di dettaglio 920
Rapporti di analisi 921
Generazione dei report Richiesta o Issue 921
Generazione dei report Area Richiesta o Categoria Issue 922
Generazione dei rapporti Priorità area Richiesta o Priorità categoria Issue 922

Capitolo 22: Gestione della conoscenza 923

Gestione della conoscenza 923

Ricerca di procedure per la gestione della conoscenza 924
Conoscenza e Multi-Tenancy 924
Modalità di impostazione di un archivio della conoscenza 925
Importazione di dati della conoscenza di esempio 926
Monitoraggio dell'archivio della conoscenza 926
Reindicizzazione dell'archivio della conoscenza 926
Indicizzazione e deindicizzazione di impostazioni della coda per l'elaborazione batch e istantanea 927
Modalità di utilizzo dei documenti dell'archivio della conoscenza 928
Inoltro conoscenza da CA SDM 930
Invio della conoscenza dalla sezione self-service 930
Attributi documento 930
Autorizzazioni del documento 931
Modifica della risoluzione 931
Preparazione pubblicazione documento 932
Pubblicazione di documenti 932
Controllo delle versioni dei documenti 933
Scadenza di documenti 934
Archiviazione ed eliminazione documenti 934
Ricerca della conoscenza 934
Chiamata del servlet CAFedSearch attraverso un servizio Web REST 935
Forum 936
Documenti della struttura Knowledge 936
Pianificazione documenti della conoscenza 936
Filtro pianificazione della conoscenza 937
visualizzazioni della pianificazione della conoscenza 939
Configurazione della visualizzazione di pianificazione 940
Accesso all'esportazione/importazione 946
Modalità di esportazione/importazione della conoscenza 947
Esportazione/importazione documenti 950
Pacchetti di esportazione/importazione 951
Visualizzazione di modelli di esportazione/importazione 952
Utilità pdm_ket—Strumento di esportazione della conoscenza 959
Utilità pdm_kit—Strumento di importazione della conoscenza 960
Consentire agli utenti di esportare e importare conoscenza 961
Servizi Web 962

Capitolo 23: Amministrazione Gestione della conoscenza 963

Amministrazione della conoscenza 963
Ricerca di procedure per l'amministrazione della conoscenza 963
Ruoli e funzioni Gestione della conoscenza 964
Interfacce utente di Gestione della conoscenza 965

Funzioni di gestione e configurazione Gestione della conoscenza 965
Opzioni della conoscenza self-service 966
Documenti e utenti 972
Come gestire i privilegi dei ruoli e la visibilità dei documenti 975
Contenuto azione 975
Visualizzazione dei contenuti azione 977
Creazione di contenuto azione (URL azione) 978
Creazione di contenuto azione (HTMPL interno) 979
Modifica del contenuto azione 979
Ricerca del contenuto azione 980
Processo di approvazione dei documenti 981
Gestione processo di approvazione 982
Definizione di un processo di approvazione per la modifica del documento 982
Creazione di un modello di processo di approvazione 984
Definizioni di stato del documento 986
Policy automatiche 988
Visualizzazione di policy automatiche 989
Modalità di impostazione delle policy automatiche 990
Creazione di una policy automatica 991
Modifica di una policy automatica 992
Pianificazione di policy automatiche 992
Visualizzazione di report relativi alle policy del ciclo di vita di un documento 993
Controllo del documento della conoscenza 993
Tipi commento 994
Modelli documento 1000
Come creare collegamenti documento della conoscenza 1007
Categorie conoscenza 1009
Report e metriche 1019
Cerca 1021
Indagine soluzione 1047
Impostazioni di sistema di Gestione della conoscenza 1050
Configurazione delle impostazioni generali 1050

Capitolo 24: Amministrazione di Support Automation 1055

Automatizzazione del supporto nel proprio ambiente 1055
Assistenza in tempo reale 1055
Amministrazione degli analisti Support Automation 1058
Introduzione 1059
Configurazione dell'assistenza in tempo reale per gli analisti 1060
Avvio dell'Assistenza in tempo reale da parte degli analisti 1069
Come configurare Assistenza in tempo reale per gli analisti 1070

Procedure utilizzabili dagli utenti finali per accedere alle sessioni di assistenza 1071
Procedure usate dagli analisti per automatizzazione il supporto per gli utenti finali 1072
Procedure utilizzate dagli analisti per fornire assistenza in tempo reale 1073
Amministrazione degli utenti Support Automation 1073
Configurazione delle autorizzazioni dei ruoli Support Automation 1074
Utenti anonimi e registrati Support Automation 1075
Configurazione di Support Automation per un utente guest 1076
Amministrazione livello di accesso Support Automation 1079
Amministrazione delle notifiche relative all'attività di Support Automation 1080
Adattamenti pagine Support Automation 1081
Amministrazione personalizzazione 1082
Amministrazione della localizzazione 1082
Configurazione del layout della pagina 1083
Proprietà di sistema Support Automation 1083
Amministrazione delle code Support Automation 1084
Gestione delle code 1084
Gestione dei riepiloghi di coda 1085
Gestione delle ore delle code 1086
Gestione dei modelli di ticket 1086
Impostazioni di amministrazione 1086
Configurazione delle impostazioni Support Automation 1087
Personalizzazione degli strumenti Support Automation 1089
Attività automatiche 1089
Amministrazione chat predefinita 1095
Credenziali predefinite 1096
Dichiarazioni di non responsabilità 1096
Amministrazione del registro sessione 1097
Visualizzazione del registro sessione 1097
Report Support Automation 1098
Ricezione di una Richiesta di ticket 1100
Invito dell'utente a una sessione di assistenza 1100
Risoluzione del ticket mediante una sessione di chat 1101
Assistenza in tempo reale 1101
Conclusione della sessione di assistenza e chiusura del ticket 1102

Capitolo 25: Identificazione dei problemi di prestazioni in CA SDM 1105

Definizione i problemi di prestazioni 1107
Verifica dei prerequisiti 1108
Installazione degli strumenti Ps per Windows 1108
Raccolta delle informazioni dallo strumento di report diagnostico CA 1109
Esecuzione dello strumento di report diagnostico 1109

Verifica del report di Windows 1111
Verifica del report di UNIX 1112
Verifica del report diagnostico dei dati raccolti 1113
Raccolta dei dettagli di ambiente del server di database 1114
Raccolta dei dati sulle prestazioni dai server di CA SDM 1115
Raccolta dei dati sull'utilizzo mediante la registrazione periodica 1116
Verifica delle indicazioni di ottimizzazione 1119

Appendice A: Comandi di riferimento 1121

bop_sinfo--Visualizzazione delle informazioni di sistema 1122
dbmonitor_nxd--Daemon monitoraggio database 1123
pdm_backup - Scrittura di tabelle di database in file ASCII 1124
pdm_cache_refresh - Aggiornamento del database 1126
pdm_configure - Apertura della finestra di configurazione 1127
pdm_d_refresh - Avvio dei daemon con errori 1128
pdm_deref - Annullamento del riferimento (dati in formato ASCII) 1128
pdm_discimp - Importazione degli asset rilevati 1132
pdm_discupd -- Aggiornamento asset rilevati 1134
pdm_extract - Estrazione dei dati dal database 1134
pdm_halt - Arresto dei daemon o dei servizi 1138
pdm_init - Avvio dei daemon 1138
pdm_key_refresh - Aggiornamento delle informazioni chiave nella cache 1139
pdm_lexutil--Modifica del dizionario di CA SDM 1139
pdm_k_reindex—Utilità di reindicizzazione della conoscenza 1140
Modalità di utilizzo di pdm_k_reindex 1141
Tracciamento del processo di reindicizzazione 1142
Importazione e reindicizzazione 1143
Indicizzazione e deindicizzazione di impostazioni della coda per l'elaborazione batch e istantanea 1143
pdm_listconn - Elenco delle connessioni attive 1144
pdm_load - Aggiunta, aggiornamento ed eliminazione dei record del database 1146
pdm_logfile - Modifica delle dimensioni cutover del file stdlog 1148
Utilità pdm_log4j_config - Modifica del file delle proprietà log4j 1149
Esempi di uso dell'utilità 1151
Modifica manuale dell'intervallo di aggiornamento del file di registro 1152
Modifica dell'appender jsrvr.log 1153
Modifica dell'appender jstd.log 1153
pdm_proctor_init - Avvio di proctor sui server secondari 1154
pdm_replace - Sostituzione di una tabella di database 1154
Gestione dell'applicazione dei servizi Web RESTful di CA SDM - pdm_rest_util 1156
Annullamento della distribuzione dell'applicazione dei servizi Web REST 1157
pdm_restore - Ripristino di un database 1157

pdm_status - Stato dei daemon e dei processi 1159
pdm_task - Impostazione delle variabili di ambiente 1159
Interfaccia riga di comando di Text API - pdm_text_cmd 1160
Esempi di input....1162
pdm_uconv - Conversione di set di caratteri in UTF-8 1163
pdm_userload - Aggiunta, aggiornamento ed eliminazione dei record del database 1166
pdm_webstat - Statistiche sull'uso del Web 1169
report - Generazione dei rapporti 1173
rpt_srv - Generazione dei rapporti....1174
uniconv - Avvio del daemon convertitore eventi CA NSM UNIX 1175
Utilità pdm_mail - Invio di informazioni di posta elettronica 1176
Utilità pdm_server_control--Identificazione dei server 1179

Appendice B: Descrizione dei campi delle visualizzazioni 1181

Descrizione dei campi delle visualizzazioni 1182
View_Act_Log....1182
View_Audit_Assignee....1183
View_Audit_Group....1184
View_Audit_Priority 1185
View_Audit_Status....1185
View_Change_Act_Log....1186
View_Change....1187
View_Change_to_Assets 1192
View_Change_to_Change_Act_Log 1193
View_Change_to_Change_WF....1194
View_Change_to_Properties 1196
View_Contact_Full 1197
View_Contact_to_Environment....1200
View_Group 1200
View_Group_to_Contact....1201
View_Issue 1202
View_Issue_Act_Log....1206
View_Issue_to_Assets....1207
View_Issue_to_Issue_Act_Log 1208
View_Change_to_Request 1209
View_Issue_to_Issue_WF....1212
View_Issue_to_Properties 1214
View_Request 1215
View_Request_to_Act_Log 1221
View_Request_to_Properties 1221

Capitolo 1: Introduzione

Questa sezione contiene i seguenti argomenti:

Destinatari (a pagina 25)
Informazioni necessarie (a pagina 25)
Processi e procedure ottimali per la gestione dei servizi (a pagina 26)

Destinatari

Questa guida è destinata all'amministratore di CA Service Desk Manager (CA SDM) ovvero la persona responsabile dell'amministrazione del prodotto. Alcune delle attività che l'amministratore esegue sono riportate di seguito:

- Avvio e arresto dei servizi necessari al server CA SDM.
- Configurazione dei vari componenti di sistema.
- Identificazione delle opzioni disponibili per gli utenti.
- Generazione dei rapporti in base ai dati del service desk.

Lo scopo di questa guida è quello di consentire l'utilizzo di CA SDM per implementare, gestire e applicare il supporto dei servizi. Questa guida aiuta a comprendere in che modo il prodotto riesca a risolvere le sfide legate all'automazione e alla gestione dell'erogazione dei servizi, dall'individuazione del problema fino alla relativa risoluzione.

Informazioni necessarie

Per amministrare CA SDM, è consigliabile avere familiarità con quanto riportato di seguito:

- Il sistema operativo in cui è installato CA SDM
- Il funzionamento del server Web
- Le attività di amministrazione di base

Questa guida presuppone che il prodotto sia stato installato correttamente, sulla base delle informazioni contenute nella *Guida all'implementazione*.

Processi e procedure ottimali per la gestione dei servizi

L'implementazione di processi standardizzati e procedure ottimali ha un effetto diretto sull'efficacia, sulla produttività e sui costi dell'ambiente di supporto dei servizi. CA fornisce una libreria di processi e procedure ottimali consigliati per la gestione dei servizi, conformi agli standard del settore e riconosciuti, che includono ITIL, CobIT, BS15000 e così via. I processi descritti per CA SDM includono:

- Gestione degli incidenti
- Gestione dei problemi
- Gestione dei Cambiamenti
- Gestione richieste
- Gestione della configurazione
- Gestione versione
- Gestione della conoscenza
- Support Automation

Nota: le informazioni sulla libreria Best Practices sono disponibili in linea. Per ulteriori informazioni sulla libreria Best Practices per la gestione dei servizi di CA, inclusi white paper e altra documentazione, visitare il sito Web http://www.ca.com/sm/bp http://www.ca.com/sm/bp. I partner di CA esperti di processi strategici possono aiutare a personalizzare la libreria delle procedure ottimali in base alle necessità dell'organizzazione.

Capitolo 2: Gestione dei server

Questa sezione contiene i seguenti argomenti:

Numero di server (a pagina 27)
Modalità di modifica di una configurazione server (a pagina 28)
Modalità di avvio dei server di CA SDM (a pagina 28)
Esecuzione della manutenzione progressiva sui server di CA SDM (a pagina 32)
Modalità di configurazione dell'autenticazione SSL (a pagina 38)
Modalità di configurazione di TCP/IP (a pagina 48)
Modalità di distribuzione dei servizi Web CMDBf (a pagina 49)
Modalità di riavvio dei server CA SDM (a pagina 49)
Modalità di arresto dei server di CA SDM (a pagina 52)
Supporto di tablet (a pagina 56)
Accesso a Tomcat (a pagina 58)
Interfaccia PDA (a pagina 59)
Registrazione REST (a pagina 60)
Configurazione dei processi per i server di CA SDM (a pagina 67)

Numero di server

L'installazione di CA SDM include uno o più componenti server che l'amministratore può gestire. Il numero di server dipende dalla configurazione di CA SDM:

- Convenzionale: un server primario e uno o più server secondari.
- Disponibilità avanzata: un server in background, uno o più server di standby e uno o più server applicazioni.

Dopo l'installazione di CA SDM, configurare ogni computer in cui vengono eseguiti i componenti del prodotto. È possibile eseguire la configurazione del server durante il processo di installazione oppure in seguito. È necessario riavviare i servizi di CA SDM dopo aver modificato la configurazione del server.

Per informazioni su come pianificare e configurare i server, consultare la *Guida all'implementazione*.

Modalità di modifica di una configurazione server

In qualità di amministratore, è possibile configurare tutti i server dell'installazione di CA SDM. Il numero e il tipo di server dipendono dalla configurazione di CA SDM: La configurazione iniziale viene eseguita durante il processo di installazione di CA SDM.

Nota: eventuali modifiche all'ambiente di sistema potrebbero richiedere modifiche della configurazione del server. Ad esempio, modifiche del sistema di gestione dei database o dell'integrazione con CA EEM o con un server Web come Tomcat.

È possibile utilizzare l'utilità di configurazione per apportare modifiche a una configurazione del server. Per ulteriori informazioni sulla configurazione del server, consultare la *Guida all'implementazione*.

Procedere come descritto di seguito:

1. Accedere al server che si desidera configurare nuovamente.
2. Dal menu Start di Windows, selezionare Programmi, CA, CA SDM, Configurazione.

   Viene visualizzata l'utilità di configurazione di CA SDM.
3. Compilare i campi dell'utilità e fare clic su Avanti.

   Il pannello di destra mostra i campi corrispondenti al collegamento evidenziato nel riquadro di navigazione sulla sinistra.
4. Proseguire seguendo le istruzioni visualizzate per completare l'installazione, quindi fare clic su Fine.

   La configurazione del server viene modificata.

Modalità di avvio dei server di CA SDM

A seconda della configurazione di CA SDM, completare le azioni seguenti:

- Avviare i server di CA SDM con la configurazione convenzionale (a pagina 30)
- Avviare i server di CA SDM con la configurazione di disponibilità avanzata (a pagina 31).

  La seguente tabella descrive i processi che vengono avviati automaticamente all'avvio dei server di CA SDM:

Processo	Descrizione
Daemon Agent (pdm_proctor_nxd)	Agente daemon responsabile dell'avvio dei daemon gestiti
Daemon Monitor (pdm_d_mgr)	Monitora i processi daemon
BOP Virtual DB (bpvirtdb_srvr)	Server di database virtuale BOP

Processo	Descrizione
Data Dictionary (ddictbuild)	Ricrea il dizionario dati ogni volta che il sistema viene avviato.
KPI Daemon (kpi_daemon)	Gestisce la raccolta, l'organizzazione e la memorizzazione dei dati KPI.
Oracle Agent (orcl_agent)	Agente per il database Oracle: numerose istanze, in base alla quantità di dati
Oracle DB (orcl_prov_nxd)	Provider del database Oracle
SQL Agent (sql_agent) (viene eseguito solo se si utilizza MS SQL)	Agente per il database SQL Server: numerose istanze, in base alla quantità di dati
SQL DB (sql_prov_nxd) (viene eseguito solo se si utilizza MS SQL)	Provider del database Microsoft SQL Server
Event Manager (ehm_nxd)	Gestione degli eventi
Message Dispatcher (sslump_nxd)	Invia i messaggi
Notification Manager (bpnotify_nxd)	Gestisce le notifiche
Object Engine (domsrvr)	Gestione oggetti CA SDM
Report Manager (pcrpt_nxd)	Per le segnalazioni al PC
Software Version Control (pdm_ver_nxd)	Gestisce le versioni dei componenti di sistema specificati
Method Engine (spel_srvr)	Server di interpretazione del codice ortografia
Text API (pdm_text_nxd)	Daemon dell'API di testo per le interfacce di posta elettronica e CA NSM
Timed Events/Notifications (animator_nxd)	Eventi e notifiche temporizzati
User Validation (boplgin)	Validazione account utente
User Authentication (bopauth)	Autenticazione account utente
Web Engine (webengine)	Esegue il motore per il client Web
Archive Purge Daemon (arcpur_srvr)	Gestisce l'elaborazione in background dell'archiviazione e dell'eliminazione
BU Daemon (bu_daemon)	Gestisce il calcolo della classificazione FAQ per i documenti della conoscenza
DB Monitor (dbmonitor_nxd)	Monitora le tabelle comuni CA relativamente alle modifiche
EBR Daemon (bpebr_nxd)	Gestisce le richieste di ricerca conoscenza
EBR Idx Daemon (bpeid_nxd)	Gestisce la indicizzazione/reindicizzazione delle parole chiave EBR

Processo	Descrizione
KRC Daemon (krc_daemon)	Gestisce le notifiche e i calcoli statistici per la Scheda report della conoscenza
KT Daemon (kt_daemon)	Gestisce i documenti della conoscenza (notifiche, autorizzazioni, processo di approvazione KD e così via)
LDAP virtdb (ldap_virtdb)	Agente per le comunicazioni con i server LDAP
Mail Daemon (pdm_mail_nxd)	Gestisce le notifiche di posta elettronica in uscita
Mail Eater (pdm_maileater_nxd)	Gestisce le notifiche di posta elettronica in arrivo
MDB Registration Server (mdb_registration_nxd)	Agente per la gestione delle richieste di registrazione MDB
PDM RPC (PDM_RPC)	Gestisce le richieste dei servizi Web
Repository Daemon (rep_daemon)	Gestisce i repository degli allegati
Spell checker (lexagent_nxd)	Gestisce le richieste per il controllo ortografia
Time-to-Violation (ttv_nxd)	Strumento per la previsione delle violazioni SLA
tomcat controller (pdm_tomcat_nxd)	Gestisce i servizi Tomcat

Nota: in questa tabella, il processo di gestione delle notifiche è valido solo per l'ambiente Windows e il processo relativo al DB predefinito è valido solo per l'ambiente UNIX.

Avvio dei server di CA SDM con la configurazione convenzionale

Avviare i server nell'ordine seguente:

1. Avviare il server secondario (a pagina 30).
2. Avviare il server primario (a pagina 31).

Avvio del server secondario

Se l'installazione include uno o più server secondari, è necessario avviarli prima di avviare il server primario.

Procedere come descritto di seguito:

- (Windows) Selezionare Servizi dal Pannello di controllo, selezionare il servizio Proctor remoto CA SDM e fare clic su Inizio.
- (UNIX) Usare pdm_init dalla riga di comando.

Ulteriori informazioni:

pdm_proctor_init - Avvio di proctor sui server secondari (a pagina 1154)

Avvio del server primario

In ogni installazione di CA SDM è presente un server primario che gestisce le funzioni di base del prodotto.

Importante: Se l'installazione include uno o più server secondari, è necessario avviare i server secondari (a pagina 30) prima di avviare il server primario.

Procedere come descritto di seguito:

- (Windows) Selezionare Pannello di controllo, il servizio Server CA SDM e fare clic su Inizio. Se necessario, è possibile avviare manualmente il servizio oppure configurarlo per l'avvio automatico come qualsiasi altro servizio di Windows.
- (UNIX) Usare pdm_init dalla riga di comando.

Avviare i server di CA SDM con la configurazione di disponibilità avanzata.

Avviare i server nell'ordine seguente:

Nota: (Windows) Selezionare Pannello di controllo, il servizio Server CA SDM e fare clic su Inizio. Se necessario, è possibile avviare manualmente il servizio oppure configurarlo per l'avvio automatico come qualsiasi altro servizio di Windows. (UNIX) Usare pdm_init dalla riga di comando.

1. Avviare il server in background.
2. Avviare i server di standby e il server applicazioni (in qualsiasi ordine).

Esecuzione della manutenzione progressiva sui server di CA SDM

In qualità di amministratori di sistema, è possibile eseguire la manutenzione server progressiva sui server di CA SDM. È possibile eseguire questa manutenzione per applicare le patch o eseguire una manutenzione generale sui server. Si consiglia di eseguire la manutenzione su tutti i server in un ordine specifico. Questo processo assicura che tutti i server vengano aggiornati con le modifiche, con una minima o nessuna interruzione del servizio per gli utenti finali. Per qualsiasi modifica di server specifica, non è necessario aggiornare tutti gli altri server.

Importante: Prima di applicare una patch MDB comune, una patch di sistema operativo o di protezione, verrà richiesto di arrestare tutti i server di CA SDM. In tal caso, l'attività dell'utente viene interrotta e l'accesso a CA SDM viene impedito finché tutti i server sono attivi e in esecuzione. Si consiglia che l'amministratore di sistema pianifichi l'applicazione della patch di conseguenza.

Il diagramma seguente mostra il processo consigliato per eseguire una manutenzione progressiva sui server di CA SDM:

Nota: A seconda degli standard dell'organizzazione, il processo di manutenzione progressiva nella propria organizzazione può differire dal processo consigliato.

(Consigliato) Esecuzione della manutenzione progressiva sui server CA SDM
Admin
Verifica delle considerazioni
Promozione del server di standby come nuovo server in backgroung
Esecuzione della manutenzione progressiva sul server in background precedente
Avvio del server in background precedente
Promozione del server in background precedente come nuovo server in background
Esecuzione della manutenzione progressiva sul server di standby
Esecuzione della manutenzione progressiva sui server applicazioni

Procedere come descritto di seguito:

1. Verificare le considerazioni (a pagina 34).
2. Arrestare il server di standby (che si desidera promuovere come nuovo server in background).
3. Eseguire la manutenzione progressiva sul server di standby.
4. Eliminare il controllo versioni tra il server di standby e il server in background (a pagina 35).
5. Avviare il server di standby.
6. Promuovere il server di standby a nuovo server in background (a pagina 35).
7. Eseguire la manutenzione progressiva sul server in background precedente.
8. Avviare il server in background precedente.

   Quando si avvia il server in background, questo diventa un server di standby.
9. Eseguire la manutenzione progressiva su tutti gli altri server di standby.

   Nota: Arrestare il server di standby, eseguire la manutenzione progressiva e avviare il server.
10. Eseguire la manutenzione progressiva sui server applicazioni (a pagina 36).

Verifica delle considerazioni

Durante un failover del server in background verso il server di standby, considerare quanto segue:

- I nuovi utenti non possono accedere.
- Per gli utenti già connessi, le azioni seguenti non funzionano durante il failover, pertanto è necessario eseguire un nuovo tentativo dopo il failover:
  - Creazione di ticket con allegati.
  - Download degli allegati.
  - Ricerca dei documenti della conoscenza.
  - Indicizzazione dei nuovi documenti della conoscenza.
  - Messaggio di posta elettronica in entrata.
  - Gli eventi SLA che non vengono attivati fino al completamento del failover.

Importante. Se lo strumento di terze parti è stato configurato per abilitare il failover automatico dei server CA SDM, è necessario disattivarlo prima di avviare la manutenzione progressiva.

Eliminazione del controllo versioni tra il server di standby e il server in background

Il controllo versioni di CA SDM consente di gestire le personalizzazioni del sistema su tutti i server di CA SDM. Assicurarsi di eliminare il controllo versioni sul server di standby prima di avviarlo. Questo processo assicura che il server di standby non venga aggiornato con le personalizzazioni di sistema del server in background. Per eliminare il controllo versioni, eseguire il comando seguente sul server di standby di cui si è eseguito l'aggiornamento:

```
pdm_server_control -v
```

Promozione del server di standby come nuovo server in background

Prima di arrestare il server in background, promuovere il server di standby (di cui si è eseguito l'aggiornamento) a nuovo server in background. Se Support Automation è installato con CA SDM, informare gli utenti di Support Automation attivi dell'arresto del server in background.

Procedere come descritto di seguito:

1. Eseguire il comando seguente sul server in background per avvisare tutti gli utenti attivi che utilizzano Support Automation di salvare il proprio lavoro:

   ```
   sa_server_notifier [-h] | [-q seconds] | [-c]
   ```

   -h

   Visualizza la pagina della Guida.

   -q seconds

   Questa opzione avvisa un server locale (background) di rimanere inattivo durante un intervallo di tempo specificato. Questo intervallo è il numero di secondi che trascorrono prima che il server diventi non in linea. Non è possibile utilizzare questa opzione per un server di standby o un server applicazioni.

   -c

   Questa opzione annulla una richiesta di disattivazione inviata precedentemente.

   Un messaggio popup viene visualizzato a tutti gli utenti attivi che utilizzano Support Automation. Questo messaggio comunica agli utenti l'arresto del server e il tempo rimasto prima dell'arresto. Gli utenti devono salvare il proprio lavoro e uscire entro il tempo pianificato.

2. Eseguire il comando seguente sul server di standby che si desidera promuovere a nuovo server in background:

   ```
   pdm_server_control -b
   ```

   -b

   Indica a un server di standby locale di diventare il server in background. Il server di standby deve essere già in esecuzione. Se il server non è in esecuzione, viene avviato ma non viene eseguito nessun failover. Per avviare un failover, eseguire di nuovo il comando.

   Il server in background si arresta automaticamente e il server di standby viene promosso a nuovo server in background. Questo cambiamento non interessa le sessioni dell'utente finale. Gli eventuali aggiornamenti in corso vengono archiviati e ritardati, finché il nuovo server in background non passa in linea.

Esecuzione della manutenzione progressiva sui server applicazioni

Come procedura consigliata, è possibile eseguire prima la manutenzione progressiva su un server applicazioni a cui sono connessi pochi utenti o nessun utente. Informare quindi tutti gli utenti attivi su altri server applicazioni di accedere al server aggiornato. Infine, è possibile eseguire la manutenzione sugli altri server applicazioni. Questo processo assicura che gli utenti non vengano spostati tra server applicazioni più volte.

Procedere come descritto di seguito:

1. Scegliere il server applicazioni meno attivo (a pagina 36).
2. Arrestare il server applicazioni meno attivo, eseguire la manutenzione progressiva e avviarlo.

   Il server applicazioni viene aggiornato con tutte le modifiche.
3. Arrestare l'altro server applicazioni (a pagina 37).
4. Eseguire la manutenzione progressiva sul server applicazioni e avviarlo.

   Il server applicazioni viene aggiornato con tutte le modifiche.
5. Eseguire le fasi 3 e 4 per gli altri server applicazioni.

   Tutti i server applicazioni vengono aggiornati con tutte le modifiche.

Scegliere il server applicazioni meno attivo

Scegliere un server applicazioni con l'attività utente più bassa. Eseguire il comando seguente su ciascun server applicazioni per scegliere quello con il numero più basso di sessioni attive o con nessuna sessione attiva.

```
pdm_webstat
```

Nota: Questo comando non acquisisce le sessioni SOAP o del servizio Web REST.

Arresto dell'altro server applicazioni

Tutti gli utenti attivi su un server applicazioni vengono informati di spostarsi sul server applicazioni meno attivo prima di arrestarlo. Assicurarsi di avere riavviato il server applicazioni meno attivo prima di spostare tutti gli utenti su di esso.

Procedere come descritto di seguito:

1. (Consigliato) Informare tutti gli analisti di Support Automation attivi sul server applicazioni che si desidera arrestare di creare un ticket in CA SDM con le informazioni sulla sessione. Questo processo assicura che le informazioni sulla sessione non vengano perse. Ad esempio, l'analista di Support Automation si trova in una sessione con un cliente per risolvere un problema di hardware. In tale caso, l'analista di Support Automation può creare un problema in CA SDM con le informazioni sulla sessione prima che il server applicazioni venga arrestato.
2. Inviare una notifica (ad esempio, una notifica di posta elettronica) a tutti gli utenti attivi sul server applicazioni perché si spostino sul server applicazioni meno attivo che è stato appena riavviato. Questa notifica può includere i dettagli del server applicazioni aggiornato.
3. Eseguire il comando seguente sul server applicazioni:

   ```
   pdm_server_control [-h] -q interval -s server_name
   ```

   -h

   Visualizza la pagina della Guida.

   -q interval -s server_name

   Notifica a un server applicazioni locale o remoto di rimanere inattivo in un intervallo di tempo specificato. Questo intervallo è il numero di secondi prima che il server diventi non in linea. Quando si utilizza questa opzione senza un server_name, il server locale viene informato di rimanere inattivo. Non è possibile utilizzare questa opzione per un server in background o di standby.

   Tutti gli utenti attivi sul server applicazioni visualizzano un messaggio popup che li informa dell'arresto del server e del tempo rimasto prima dell'arresto. Gli utenti devono salvare il proprio lavoro e uscire entro il tempo indicato. Il server applicazioni si arresta dopo il tempo specificato. Gli utenti accedono all'altro server applicazioni per riprendere il lavoro. L'analista di Support Automation può fare riferimento al ticket e riprendere il lavoro.

   L'arresto del server applicazioni è riuscito.

Modalità di configurazione dell'autenticazione SSL

In qualità di amministratori di sistema, è possibile configurare Web Director per indirizzare le richieste di accesso a un motore Web specifico mediante il protocollo SSL (Secure Socket Layer). La configurazione dell'autenticazione SSL fornisce una maggiore protezione dell'accesso consentendo allo stesso tempo agli utenti di accedere a una connessione con prestazioni più elevate.

Equation 1: Configurazione dell'autenticazione SSL per CA SDM

Ulteriori informazioni:

Impostazione della funzionalità del motore Web mediante i parametri Web Director (a pagina 39)
Configurazione dell'ambiente di accesso SSL (a pagina 42)
Scegliere l'ambiente di accesso SSL (a pagina 40)
Verifica dei prerequisiti (a pagina 39)

Verifica dei prerequisiti

Verificare i prerequisiti seguenti prima di iniziare la configurazione SSL:

- CA SDM è stato installato e configurato sul server in cui si desidera implementare il protocollo SSL.
- Almeno due motori Web sono stati configurati e assegnati a un Web Director. Per ulteriori informazioni su come configurare motori Web e Web Director, consultare lo scenario *Configurazione del processo del server per CA SDM per migliorare le prestazioni*.

Impostazione della funzionalità del motore Web mediante i parametri Web Director

Dopo che si è configurato il motore Web per utilizzare un Web Director, il motore Web può gestire le richieste dei client Web. Il motore Web può gestire le richieste di accesso (e reindirizzare i non accessi altrove) o le richieste di non accesso (e reindirizzare gli accessi altrove) o ambedue (motore Web con scopo generale). Il parametro di WebDirector trovato nel file <Host_Name>-web[#].cfg determina come il motore Web può gestire le richieste di accesso.

La tabella seguente mostra la relazione tra il ruolo del motore Web e l'impostazione dei parametri di Web Director:

Funzionalità del motore Web	Impostazioni parametro ‘webdirector’ ‘<nome_host>-web[#].cfg’
Gestione richieste di accesso	‘UseDirector AfterLogin’; ‘Willingness 0’
Gestione attività non di accesso	‘UseDirector BeforeLogin’; ‘Willingness [1 thru 10]’
Scopo generale	‘UseDirector Yes’; Willingness [1-10]’

Scegliere l'ambiente di accesso SSL

È possibile utilizzare Web Director per un accesso SSL in un ambiente Web SSL/non SSL misto per reindirizzare ogni richiesta di accesso Web ai motori Web SSL specifici. Tutte le altre richieste possono essere reindirizzate e gestite da motori Web non SSL.

Scegliere tra gli ambienti di accesso dello SSL seguenti:

- Ambiente non SSL con bilanciamento del carico base
- Ambiente SSL globale con bilanciamento del carico base
- Accesso in un ambiente non SSL con bilanciamento del carico opzionale
- Accesso in un ambiente SSL misto con bilanciamento del carico opzionale

Ambiente non SSL con bilanciamento del carico base

È possibile utilizzare il Web Director in un ambiente non SSL con un bilanciamento del carico di base. Web Director bilancia il carico su tutti i motori Web in base al valore del parametro disponibilità di ciascun motore Web. Ogni motore Web può gestire le richieste di accesso e non di accesso. Il protocollo HTTP viene utilizzato per le comunicazioni tra il client Web e il server Web.

Per ciascun motore Web controllato da Web Director, impostare i parametri webdirector nel file "<*nome_host*>-web[*#*].cfg" del motore Web nel modo seguente:

- UseDirector: Yes
- WebDirectorSlumpName: (non modificare questo valore)
- WillingnessValue: [da 1 a 10]
- RedirectingURL: (il valore del protocollo aggiunto preventivamente può essere mancante o http)

Ambiente SSL globale con bilanciamento del carico base

È possibile utilizzare il Web Director in un ambiente SSL globale con un bilanciamento del carico di base. Web Director bilancia il carico su tutti i motori Web in base al valore del parametro disponibilità di ciascun motore Web. Ogni motore Web può gestire le richieste di accesso e non di accesso. Il protocollo HTTPS deve essere utilizzato per tutte le comunicazioni tra i client Web e il server Web.

Per ciascun motore Web controllato da Web Director, impostare i parametri webdirector nel file "<*nome_host*>-web[*#*].cfg" del motore Web nel modo seguente:

- UseDirector: Yes
- WebDirectorSlumpName: (non modificare questo valore)

- WillingnessValue: [da 1 a 10]
- RedirectingURL: (il valore del protocollo aggiunto preventivamente deve essere https)

Accesso in un ambiente non SSL con bilanciamento del carico opzionale

È possibile utilizzare il Web Director per l'accesso in un ambiente non SSL con un bilanciamento del carico di base. Il motore Web di tipo "solo richieste di accesso" gestisce solo le richieste di accesso. I restanti motori Web controllati da Web Director gestiscono tutte le altre richieste. Questo tipo di configurazione assegna l'intero onere della gestione delle richieste di accesso ai motori Web di tipo "solo richieste di accesso". Il protocollo HTTP viene utilizzato per le comunicazioni tra il client Web e il server Web.

Per i motori Web di tipo "solo richieste di accesso", impostare i parametri webdirector nel file "<*nome_host*>-web[*#*].cfg" del motore Web nel modo seguente:

- UseDirector: AfterLogin
- WebDirectorSlumpName: (non modificare questo valore)
- WillingnessValue: 0
- RedirectingURL: (il valore del protocollo aggiunto preventivamente può essere mancante o http)

Per i motori Web di tipo "non di accesso", impostare i parametri webdirector nel file "<*nome_host*>-web[*#*].cfg" del motore Web nel modo seguente:

- UseDirector: Before Login
- WebDirectorSlumpName: (non modificare questo valore)
- WillingnessValue: [da 1 a 10]
- RedirectingURL: (il valore del protocollo aggiunto preventivamente può essere mancante o http)

Accesso in un ambiente SSL misto con bilanciamento del carico opzionale

È possibile utilizzare il Web Director per l'accesso SSL in un ambiente SSL/non SSL con bilanciamento del carico opzionale. Ogni richiesta di accesso Web viene reindirizzata e gestita dai motori Web SSL, mentre altre richieste vengono gestite dai motori Web non SSL. Il protocollo HTTPS deve essere utilizzato per tutte le comunicazioni tra il client Web e i motori Web SSL.

Configurazione dell'ambiente di accesso SSL

La configurazione del protocollo SSL consente la crittografia delle transazioni Web, garantendo la massima protezione dei dati riservati, in particolar modo delle password. A seconda del tipo di configurazione, è possibile implementare un ambiente di accesso SSL sui server di CA SDM configurati.

Procedere come descritto di seguito::

1. Accedere al server seguente, a seconda della configurazione di CA SDM:
   - Disponibilità avanzata: server applicazioni
   - Convenzionale: server primario o secondario
2. Verificare che il server abbia importato correttamente un certificato SSL.
3. Creare una copia (con le relative sottodirectory) della directory '$NX_ROOT/bopcfg/www/wwwroot' e assegnarle il nome seguente:

   ‘$NX_ROOT/bopcfg/www/wwwrootsec’
4. Aggiungere una nuova directory virtuale per il server Web chiamata CAisdsec.
5. Associare la directory virtuale alla directory fisica seguente:

   ‘$NX_ROOT/bopcfg/www/wwwrootsec’
6. Verificare che le autorizzazioni della directory virtuale per CAisdsec corrispondano alle autorizzazioni della directory virtuale CAisd per l'esecuzione degli script. Abilitare il protocollo SSL per la directory virtuale CAisdsec.

   Nota: in questo esempio, CAisdsec è definita dall'utente e può essere rinominata.
7. Salvare le modifiche.

   Nota: I Web Director non utilizzano il file ‘<Host_Name>-web[#].cfg’. I motori Web, invece, richiedono un file '<nome_host>-web[#].cfg' univoco. Durante l'esecuzione della configurazione, vengono generati automaticamente dei file web.cfg di esempio. È possibile importare le personalizzazioni del file web.cfg originale nei nuovi file di configurazione Web specificando il file web.cfg originale come file modello.
8. Copiare e salvare copie di backup dei file seguenti, che possono essere utili nel caso si desideri ripristinare l'ambiente originale:
   - $NX_ROOT/pdmconf/pdm_startup.tpl
   - $NX_ROOT/pdmconf/pdm_startup
   - $NX_ROOT/bopcfg/www/web.cfg file
   - Qualsiasi file primary-web[#].cfg esistente
   - $NX_ROOT/bopcfg/www/CATALINA_BASE/webapps/CAisd/WEB-INF/web.xml e web.xml.tpl

- Per la configurazione di un server secondario, salvare le copie di backup di tutti i file esistenti $NX_ROOT/bopcfg/www/web.cfg o <Secondary_Server_Host_Name>-web[#].cfg e $NX_ROOT/bopcfg/www/CATALINA_BASE/webapps/CAisd/WEB-INF/web.xml*

9. Per ciascun motore Web assegnato a un Web Director, assicurarsi che i parametri '(<Host_Name>-web[#].cfg 'webdirector') del motore Web siano impostati correttamente esaminando il file in un editor di testo. Se necessario, modificare i valori del parametro 'webdirector' in modo che riflettano il ruolo del motore Web desiderato. Quindi copiarli nella directory: $NX_ROOT/bopcfg/www.

10. Spostare tutti i file $NX_ROOT/samples/pdmconf/primary-web[#].cfg nella directory $NX_ROOT/bopcfg/www.

    Per la configurazione del server secondario, spostare tutti i file $NX_ROOT/samples/pdmconf/'secondary_server_name-web[#].cfg' dal server primario alla directory $NX_ROOT/bopcfg/www del server secondario.

11. Se si utilizza un server servlet come Tomcat, CA SDM crea file web.xml che possono sostituire il file web.xml su ciascun server che ospita un motore Web. Questi file sono chiamati primary-web.xml. Rinominare i file e copiarli nella directory: $NX_ROOT/bopcfg/www/CATALINA_BASE/webapps/CAisd/WEB-INF.

    Se si utilizza un server HTTP quale IIS o Apache, è necessario creare copie del file pdmweb.exe nella directory $NX_ROOT/bopcfg/www/wwwroot, un file pdmweb[#].exe per ciascun motore Web e un file pdmweb_d[#].exe per ciascun Web Director che è stato configurato. Accertarsi che i nomi assegnati a pdmweb[#].exe e pdmweb_d[#].exe siano conformi ai valori CGI I/F appropriati (ad esempio, pdmweb1.exe, pdmweb2.exe, pdmweb_d1.exe e così via).

12. Se si utilizza IIS e si desidera aggiungere le estensioni del server per ogni interfaccia CGI, è possibile copiare il file primary-site.dat nella directory locale $NX_ROOT/bopcfg/www come site.dat. Quando il sistema viene riconfigurato, queste estensioni in locale vengono aggiunte a IIS.

13. Riconfigurare il server primario senza reinizializzare il database e avviare i servizi.

14. Dopo la riconfigurazione, verificare la validità delle impostazioni correnti. Avviare i daemon di CA SDM. Verificare che non vi siano errori nei file stdlog. Utilizzare pdm_status per visualizzare i daemon e il loro stato. Utilizzare http://localhost:8080/CAisd/pdmweb.exe per accedere al sistema.

15. Per l'integrazione tra Gestione della conoscenza e CA SDM, se il protocollo SSL è stato attivato per CA SDM, è necessario cambiare il valore del protocollo dell'URL di CA SDM.

    a. In Strumenti della conoscenza, Gestione impostazioni, Generale, Integrazione, modificare il valore del protocollo dell'URL di CA SDM da http in https.

    b. Salvare e uscire.

16. Aprire la pagina di accesso a CA SDM in un browser Web, quindi verificare che un utente possa accedere e venga rispettato il comportamento previsto per il reindirizzamento/l'accesso.

Implementazione dell'ambiente di accesso SSL

Per implementare l'accesso SSL che è stato configurato, modificare i valori dei parametri di Web Director.

Procedere come descritto di seguito:

1. Per i motori Web di accesso protetto, modificare il file <nome_host>-web[#].cfg nel modo seguente:
   a. Modificare il valore del parametro CAisd da /CAisd a /CAisdsec.
   b. Modificare il valore del parametro UseDirector da Yes ad AfterLogin se Web director utilizza l'autenticazione pass-through.
   c. Modificare il valore del parametro Willingness da 5 a 0.
   d. Verificare che il valore del protocollo RedirectingURL sia riportato come HTTPS.
   e. Cambiare il valore di RedirectingURL <cgi directory> da CAisd a CAisdsec.
   f. Salvare le modifiche.
2. Per motori Web non sicuri che gestiscono tutte le altre attività, modificare i file <Host_Name>-web[#].cfg come segue:
   a. Verificare che il valore del parametro CAisd sia /CAisd.
   b. Modificare il valore del parametro UseDirector da Sì a BeforeLogin.
   c. Mantenere il valore di Willingness su 5 oppure impostarlo su un valore intero compreso tra 1 e 10, in base al carico desiderato.
   d. Verificare che il protocollo del valore RedirectingURL sia riportato come https.
   e. Verificare che il valore di RedirectingURL <directory cgi> sia CAisd.
   f. Salvare le modifiche.

      Dopo la configurazione, riavviare Service Desk. Dopo che il servizio è stato riavviato, verificare l'accesso accedendo al motore Web non SSL mediante HTTP. Verificare se si viene reindirizzati al motore Web sicuro HTTPS per l'accesso. Una volta effettuato l'accesso, si viene reindirizzati automaticamente al motore Web HTTP non SSL per le normali attività di Service Desk.

Verifica dell'ambiente di accesso SSL

È possibile verificare l'ambiente di accesso SSL per i motori Web.

Procedere come descritto di seguito:

- I motori Web di accesso protetto devono risiedere nella directory fisica associata alla directory virtuale SSL (CAisdsec in questo esempio).

  Per i motori Web di accesso protetto, creare istanze del file pdmweb.exe nella directory $NX_ROOT/bopcfg/www/wwwrootsec e assegnare loro il nome di pdmweb[#].exe. Il nome dell'eseguibile deve corrispondere al valore CGI I/F per ogni motore Web di accesso protetto.

  Esempio: Se a pdmweb2 è stato assegnato il valore CGI I/F del motore Web di accesso protetto, creare una copia fisica di pdmweb.exe e assegnarvi il nome pdmweb2.exe.

- I motori Web non protetti e i Web Director devono risiedere nella directory fisica associata alla directory virtuale non SSL CAisd.

  Per i motori Web di accesso non protetto e per i Web Director, creare nuove istanze di pdmweb.exe nella directory $NX_ROOT/bopcfg/www/wwwroot. Una copia di pdmweb.exe deve esistere per ciascun motore Web non protetto e Web Director configurato. Rinominare le copie in modo che i nuovi nomi degli eseguibili corrispondano ai valori CGI I/F definiti per i motori Web e per i Web Director.

  Esempio: Se al motore Web non protetto è stato assegnato il valore CGI I/F pdmweb3 e il valore pdmweb_d1 al Web Director, creare due copie di pdmweb.exe. Ridenominare la prima copia in pdmweb3.exe e la seconda copia in pdmweb_d1.exe.

Configurazione dell'accesso SSL per il server Tomcat

Configurare SSL sui server Tomcat nell'ambiente di CA SDM.

Procedere come descritto di seguito:

1. Per creare un archivio chiavi su ciascun server di CA SDM che richiede un certificato SSL, attenersi ai passaggi seguenti:

   Nota: Un archivio chiavi è un'unità di archiviazione per certificati, nella quale i certificati vengono importati. Tomcat indica quindi di utilizzare l'archivio chiavi e i certificati per SSL.

   a. Creare una directory nell'unità C: (o l'unità locale) con il nome certificates.

   b. Mediante la riga di comando, accedere alla directory bin JRE (per il JRE installato con Service Desk è di solito /SC/JRE)

   c. Eseguire il comando keytool -genkey -alias tomcat -keyalg RSA -keystore c:/certificates/keystore.jks.

   d. Compilare i campi in modo appropriato (prendere nota dei dati inseriti in ogni campo in quanto queste informazioni potrebbero essere richieste in seguito.).

      Un file keystore.jks viene creato nella directory C:\certificates\.

2. Generare la richiesta di certificato per ciascun server. Eseguire i passaggi seguenti per generare la richiesta di certificato:

   a. Mediante la riga di comando, accedere alla directory bin JRE (per il JRE installato con Service Desk è di solito /SC/JRE)

   b. Eseguire il comando keytool -certreq -alias tomcat -keystore c:/certificates/keystore.jks -file servername-certreq.csr

      Un file .csr viene creato nella directory c:/certificates su ciascun server in cui si è generata la richiesta di certificato.

   c. Inviare i file .csr a un vendor a scelta che genererà i certificati appropriati necessari in base a delle richiesta di certificato per ciascun server.

      Nota: Ogni certificato che si riceve da ciascun fornitore è differente. Alcuni fornitori invieranno più certificati, includendo probabilmente un certificato principale, un certificato intermedio e un certificato di autorità. Ciascun vendor ha istruzioni differenti riguardo a quali certificati da esso forniti devono essere importati nell'archivio chiavi. È consigliabile chiedere al vendor specifico utilizzato per generare i certificati le istruzioni specifiche su come importare i propri certificati nell'archivio chiavi Tomcat.

      Una volta ricevute le istruzioni specifiche dal vendor, è possibile seguirle per importare i certificati appropriati nell'archivio chiavi su ciascun server. Una volta completata questa operazione, è possibile configurare Tomcat su Service Desk in modo da indicare l'archivio chiavi in cui i certificati sono stati importati.

3. Aprire il file \bopcfg\www\CATALINA_BASE\conf\server.xml mediante un editor di testo e individuare quanto segue:

```
<-- <Connector port="8443" maxHttpHeaderSize="8192"
maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
enableLookups="false" disableUploadTimeout="true"
acceptCount="100" scheme="https" secure="true"
clientAuth="false" sslProtocol="TLS"
keystoreFile="keystoreFile="C:\Documents and Settings\user\.keystore"
keystorePass="password"/> -->
```

4. Apportare le seguenti modifiche al codice:

```
<Connector port="8443" maxHttpHeaderSize="8192"
maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
enableLookups="false" disableUploadTimeout="true"
acceptCount="100" scheme="https" secure="true"
clientAuth="false" sslProtocol="TLS"
keystoreFile="keystoreFile="C:\certs\keystore.jks"
keystorePass="password"/>
```

Nota: Assicurarsi di eliminare i tag <-- and --> che attualmente escludono il connettore HTTPS/SSL per Tomcat, quindi impostare il percorso e la password appropriati per l'archivio chiavi che si è generato all'inizio.

5. Salvare il file server.xml.

6. Riavviare Tomcat mediante i comandi seguenti:

```
pdm_tomcat_nxd –c stop
pdm_tomcat_nxd –c start
```

Nota: Si consiglia di riavviare tutti i server di CA SDM per assicurare il riavvio di Tomcat.

7. Verificare la connessione SSL di Tomcat aprendo un browser e andando all'URL di Service Desk, mediante il protocollo HTTPS e la porta di Tomcat. Ad esempio, utilizzare l'URL seguente:

```
https://servername:8080/CAisd/pdmweb.exe
```

Si apre la schermata di accesso di Service Desk. SSL su Tomcat è stato configurato correttamente.

Modalità di configurazione di TCP/IP

È possibile modificare l'impostazione TCP/IP (TCP Internet Protocol) predefinita in uno o più server. Questa impostazione non può essere applicata nel client se non è supportata nel server.

L'impostazione TCP/IP viene controllata utilizzando il file NX.env, situato nella directory $NX_ROOT. Utilizzare un editor di testo come WordPad per modificare il file. L'impostazione TCP/IP è controllata dalla seguente opzione:

NX_PROTOCOL_ONLY=*mode*

dove *mode* può essere uno dei seguenti valori:

IPv4

In modalità IPv4 vengono visualizzati i socket per i processi slump in ascolto sul traffico IPv4.

IPv6

In modalità IPv6 vengono visualizzati i socket per i processi slump in ascolto sul traffico IPv6.

Mista

In modalità mista vengono visualizzati i socket per i processi slump in ascolto sul traffico IPv4 e IPv6. A seconda della configurazione di CA SDM, è possibile configurare la modalità mista nelle circostanze seguenti:

- Convenzionale: server secondari che utilizzano un protocollo Internet diverso da quello del server primario o l'uno dall'altro.
- Disponibilità avanzata: server applicazioni che utilizzano un protocollo Internet diverso da quello del server in background o l'uno dall'altro.

Nota: se gli host IPv4 e IPv6 coesistono nella rete, verificare che siano disponibili i meccanismi, gli strumenti e le strategie di transizione necessari per il supporto di tali tecnologie prima di cambiare la configurazione del server.

Esempio

```
NX_PROTOCOL_ONLY=ipv4
```

Modalità di distribuzione dei servizi Web CMDBf

Una volta installato CA SDM, è possibile distribuire i servizi Web CMDBf.

Procedere come descritto di seguito:

1. Verificare che il server Web sia attivo e in esecuzione.
2. Accedere alla directory CMDBHOME\sdk\websvc\CMDBF.
3. Eseguire deploy_cmdbws.bat.

   I servizi Web CMDBf vengono distribuiti e avviati.

Nota: per ulteriori informazioni sulla distribuzione dei servizi Web CMDBf, consultare la *Guida di riferimento tecnico di CA CMDB*.

Modalità di riavvio dei server CA SDM

Effettuare le operazioni seguenti, in base alla configurazione di CA SDM:

- Riavviare i server di CA SDM con la configurazione convenzionale (a pagina 49).
- Riavviare i server di CA SDM con la configurazione di disponibilità avanzata (a pagina 49).

Riavvio dei server di CA SDM con la configurazione convenzionale

Per la configurazione convenzionale, si riavviano i server nell'ordine seguente:

Nota: Per riavviare un server fare clic su Start, Impostazioni, Pannello di controllo, Strumenti amministrativi, Servizi. Fare clic con il pulsante destro del mouse sul server di CA SDM e selezionare Inizio.

1. Riavviare il server secondario.
2. Riavviare il server primario.

Riavviare i server di CA SDM con la configurazione di disponibilità avanzata.

Per la configurazione di disponibilità avanzata, si consiglia di riavviare i server di CA SDM nell'ordine seguente:

Nota: Per riavviare un server fare clic su Start, Impostazioni, Pannello di controllo, Strumenti amministrativi, Servizi. Fare clic con il pulsante destro del mouse sul server di CA SDM e selezionare Inizio.

1. Riavviare tutti i server di standby.
2. Promuovere il server di standby a nuovo server in background (a pagina 35).
3. Avviare il server in background precedente.

   Quando si avvia il server in background, questo diventa un server di standby.
4. Scegliere il server applicazioni meno attivo (a pagina 36).
5. Riavviare il server applicazioni meno attivo.
6. Arrestare l'altro server applicazioni (a pagina 37).
7. Avviare il server applicazioni.
8. Eseguire i passaggi 6 e 7 per gli altri server applicazioni.

Promozione del server di standby come nuovo server in background

Prima di arrestare il server in background, promuovere il server di standby (di cui si è eseguito l'aggiornamento) a nuovo server in background. Se Support Automation è installato con CA SDM, informare gli utenti di Support Automation attivi dell'arresto del server in background.

Procedere come descritto di seguito:

1. Eseguire il comando seguente sul server in background per avvisare tutti gli utenti attivi che utilizzano Support Automation di salvare il proprio lavoro:

   ```
   sa_server_notifier [-h] | [-q seconds] | [-c]
   ```

   -h

   Visualizza la pagina della Guida.

   -q seconds

   Questa opzione avvisa un server locale (background) di rimanere inattivo durante un intervallo di tempo specificato. Questo intervallo è il numero di secondi che trascorrono prima che il server diventi non in linea. Non è possibile utilizzare questa opzione per un server di standby o un server applicazioni.

   -c

   Questa opzione annulla una richiesta di disattivazione inviata precedentemente.

   Un messaggio popup viene visualizzato a tutti gli utenti attivi che utilizzano Support Automation. Questo messaggio comunica agli utenti l'arresto del server e il tempo rimasto prima dell'arresto. Gli utenti devono salvare il proprio lavoro e uscire entro il tempo pianificato.

2. Eseguire il comando seguente sul server di standby che si desidera promuovere a nuovo server in background:

   ```
   pdm_server_control -b
   ```

   -b

   Indica a un server di standby locale di diventare il server in background. Il server di standby deve essere già in esecuzione. Se il server non è in esecuzione, viene avviato ma non viene eseguito nessun failover. Per avviare un failover, eseguire di nuovo il comando.

   Il server in background si arresta automaticamente e il server di standby viene promosso a nuovo server in background. Questo cambiamento non interessa le sessioni dell'utente finale. Gli eventuali aggiornamenti in corso vengono archiviati e ritardati, finché il nuovo server in background non passa in linea.

Scegliere il server applicazioni meno attivo

Scegliere un server applicazioni con l'attività utente più bassa. Eseguire il comando seguente su ciascun server applicazioni per scegliere quello con il numero più basso di sessioni attive o con nessuna sessione attiva.

```
pdm_webstat
```

Nota: Questo comando non acquisisce le sessioni SOAP o del servizio Web REST.

Arresto dell'altro server applicazioni

Tutti gli utenti attivi su un server applicazioni vengono informati di spostarsi sul server applicazioni meno attivo prima di arrestarlo. Assicurarsi di avere riavviato il server applicazioni meno attivo prima di spostare tutti gli utenti su di esso.

Procedere come descritto di seguito:

1. (Consigliato) Informare tutti gli analisti di Support Automation attivi sul server applicazioni che si desidera arrestare di creare un ticket in CA SDM con le informazioni sulla sessione. Questo processo assicura che le informazioni sulla sessione non vengano perse. Ad esempio, l'analista di Support Automation si trova in una sessione con un cliente per risolvere un problema di hardware. In tale caso, l'analista di Support Automation può creare un problema in CA SDM con le informazioni sulla sessione prima che il server applicazioni venga arrestato.
2. Inviare una notifica (ad esempio, una notifica di posta elettronica) a tutti gli utenti attivi sul server applicazioni perché si spostino sul server applicazioni meno attivo che è stato appena riavviato. Questa notifica può includere i dettagli del server applicazioni aggiornato.

3. Eseguire il comando seguente sul server applicazioni:

   `pdm_server_control [-h] -q *interval* -s *server_name*`

   -h

   Visualizza la pagina della Guida.

   -q interval -s server_name

   Notifica a un server applicazioni locale o remoto di rimanere inattivo in un intervallo di tempo specificato. Questo intervallo è il numero di secondi prima che il server diventi non in linea. Quando si utilizza questa opzione senza un server_name, il server locale viene informato di rimanere inattivo. Non è possibile utilizzare questa opzione per un server in background o di standby.

   Tutti gli utenti attivi sul server applicazioni visualizzano un messaggio popup che li informa dell'arresto del server e del tempo rimasto prima dell'arresto. Gli utenti devono salvare il proprio lavoro e uscire entro il tempo indicato. Il server applicazioni si arresta dopo il tempo specificato. Gli utenti accedono all'altro server applicazioni per riprendere il lavoro. L'analista di Support Automation può fare riferimento al ticket e riprendere il lavoro.

   L'arresto del server applicazioni è riuscito.

Modalità di arresto dei server di CA SDM

A seconda della configurazione CA SDM in uso, eseguire una delle azioni seguenti:

- Arrestare i server di CA SDM con la configurazione convenzionale (a pagina 52).
- Arrestare i server di CA SDM con la configurazione di disponibilità avanzata (a pagina 53).

Arrestare i server di CA SDM con la configurazione convenzionale.

Arrestare i server seguenti:

- Arrestare il server primario (a pagina 52).
- Arrestare il server secondario (a pagina 53).

(Configurazione convenzionale) Arrestare il server primario

È possibile arrestare il server primario nell'ambiente Windows o Unix.

In Windows, attenersi ai seguenti passaggi:

1. Selezionare Servizi dal Pannello di controllo.

   Viene visualizzata la finestra Servizi.

2. Selezionare il servizio CA Service Desk Manager Server e fare clic su Arresta.

   Il server primario viene arrestato. Vengono arrestati anche i processi o i daemon sui server secondari.

In UNIX, attenersi ai seguenti passaggi:

- Immettere il comando seguente nel prompt dei comandi:

  ```
  pdm_halt
  ```

  Il server primario viene arrestato. Vengono arrestati anche i processi o i daemon sui server secondari.

(Configurazione convenzionale) Arresto del server secondario

È possibile arrestare il server secondario nell'ambiente Windows o Unix.

In Windows, attenersi ai seguenti passaggi:

1. Selezionare Servizi dal Pannello di controllo.

   Viene visualizzata la finestra Servizi.

2. Selezionare il servizio CA Service Desk Manager Remote Proctor e fare clic su Arresta.

   Il server secondario viene arrestato.

In UNIX, attenersi ai seguenti passaggi:

- Immettere il comando seguente nel prompt dei comandi:

  ```
  pdm_halt
  ```

  Il server secondario viene arrestato.

Arrestare i server di CA SDM con la configurazione di disponibilità avanzata.

Arrestare i server seguenti:

- Arrestare il server di standby (a pagina 54).
- Arrestare il server in background (a pagina 54).
- Arrestare il server applicazioni (a pagina 55).

(Configurazione di disponibilità avanzata) Arresto del server di standby

È possibile arrestare il server di standby nell'ambiente Windows o Unix.

In Windows, attenersi ai seguenti passaggi:

1. Selezionare Servizi dal Pannello di controllo.

   Viene visualizzata la finestra Servizi.

2. Selezionare il servizio CA Service Desk Manager Server e fare clic su Arresta.

   Il server di standby viene arrestato.

In UNIX, attenersi ai seguenti passaggi:

- Immettere il comando seguente nel prompt dei comandi:

  ```
  pdm_halt
  ```

  Il server di standby viene arrestato.

(Configurazione di disponibilità avanzata) Arresto del server in background

Prima di arrestare il server in background, promuovere il server di standby (di cui si è eseguito l'aggiornamento) a nuovo server in background. Se Support Automation è installato con CA SDM, informare gli utenti di Support Automation attivi dell'arresto del server in background.

Procedere come descritto di seguito:

1. Eseguire il comando seguente sul server in background per avvisare tutti gli utenti attivi che utilizzano Support Automation di salvare il proprio lavoro:

   ```
   sa_server_notifier [-h] | [-q seconds] | [-c]
   ```

   -h

   Visualizza la pagina della Guida.

   -q seconds

   Questa opzione avvisa un server locale (background) di rimanere inattivo durante un intervallo di tempo specificato. Questo intervallo è il numero di secondi che trascorrono prima che il server diventi non in linea. Non è possibile utilizzare questa opzione per un server di standby o un server applicazioni.

   -c

   Questa opzione annulla una richiesta di disattivazione inviata precedentemente.

   Un messaggio popup viene visualizzato a tutti gli utenti attivi che utilizzano Support Automation. Questo messaggio comunica agli utenti l'arresto del server e il tempo rimasto prima dell'arresto. Gli utenti devono salvare il proprio lavoro e uscire entro il tempo pianificato.

2. Eseguire il comando seguente sul server di standby che si desidera promuovere a nuovo server in background:

   ```
   pdm_server_control -b
   ```

   -b

   Indica a un server di standby locale di diventare il server in background. Il server di standby deve essere già in esecuzione. Se il server non è in esecuzione, viene avviato ma non viene eseguito nessun failover. Per avviare un failover, eseguire di nuovo il comando.

   Il server in background si arresta automaticamente e il server di standby viene promosso a nuovo server in background. Questo cambiamento non interessa le sessioni dell'utente finale. Gli eventuali aggiornamenti in corso vengono archiviati e ritardati, finché il nuovo server in background non passa in linea.

(Configurazione di disponibilità avanzata) Arresto del server applicazioni

Prima di arrestare un server applicazioni, si devono informare tutti gli utenti attivi perché si spostino su un altro server applicazioni.

Procedere come descritto di seguito:

1. Inviare una notifica a tutti gli utenti attivi sul server applicazioni che si desidera arrestare perché si spostino su un altro server applicazioni. Questa notifica può includere i dettagli dell'altro server applicazioni. Ad esempio, è possibile inviare una notifica di posta elettronica.

2. Eseguire il comando seguente sul server applicazioni che si desidera arrestare:

   ```
   pdm_server_control -q interval -s server_name
   ```

   -q interval -s server_name

   Notifica a un server applicazioni locale o remoto di rimanere inattivo in un intervallo di tempo specificato. Questo intervallo è il numero di secondi che trascorrono prima che il server diventi non in linea. Utilizzando questa opzione senza un server_name, il server locale riceve la notifica di rimanere inattivo. Non è possibile utilizzare questa opzione per un server in background o di standby.

   Un messaggio popup viene visualizzato da tutti gli utenti attivi sul server applicazioni. Questo messaggio comunica agli utenti l'arresto del server e il tempo rimasto prima dell'arresto. Gli utenti devono salvare il proprio lavoro e uscire entro il tempo indicato. Il server applicazioni si arresta dopo il tempo specificato. Gli utenti accedono all'altro server applicazioni per riprendere il lavoro.

   (Consigliato) Gli analisti di Support Automation attivi possono creare un ticket collegato alla propria sessione per salvare il lavoro. Possono accedere all'altro server applicazioni e fare riferimento a questo ticket per riprendere il lavoro.

L'iPad Apple consente di visualizzare l'interfaccia Analista, le interfacce di self-service Dipendente e Vendor unicamente nel browser predefinito e con funzionalità limitate. CA SDM non supporta gli allegati sui dispositivi di tipo tablet.

Nota: Tutti gli altri tipi di tablet visualizzano l'Interfaccia Analista PDA. Su iPad, il browser Safari supporta l'interfaccia utente di CA SDM completa. L'interfaccia utente completa potrebbe essere visualizzata su iPad utilizzando altri browser, ma questi non sono inclusi nel supporto.

Accesso a Tomcat

CA SDM utilizza un file log4j.properties distinto per le proprie componenti Web come servlet e PDM_RPC. Support Automation, CMDB Visualizer e REST dispongono di un file log4j.properties separato. Per avviare o arrestare la registrazione Tomcat non è necessario riavviare i daemon di Tomcat.

L'elenco seguente descrive le differenze tra i file log4j.properties dei componenti di CA SDM:

- CA SDM controlla il file log4j.properties in NX_ROOT\site\cfg e in NX_ROOT\bopcfg\www\CATALINA_BASE\webapps\CAisd\WEB-INF per individuare eventuali cambiamenti.
- Support Automation esegue il monitoraggio del file log4j.properties in NX_ROOT\bopcfg\www\CATALINA_BASE_SA\webapps\SupportAutomation\WEB-INF.
- CMDB Visualizer esegue il monitoraggio del file cmdbvisualizerlogging.properties in NX_ROOT\bopcfg\www\CATALINA_BASE_VIZ\webapps\CMDBVisualizer\WEB-INF\classes.
- REST controlla il file rest.log4j.properties in NX_ROOT\site\cfg.

Utilizzare l'utilità pdm_log4j_config solo per modificare le variabili nei file log4j.properties, cmdbvisualizerlogging.properties e rest.log4j.properties. Non è possibile utilizzare l'utilità pdm_log4j_config per modificare l'intervallo di polling.

CA SDM verifica periodicamente i file delle proprietà log4j per rilevare le eventuali modifiche. Configurare l'intervallo di tempo modificando la variabile NX_LOG4J_REFRESH_INTERVAL nel file NX.env.

Impostazioni predefinite del servlet

I servlet seguenti eseguono la registrazione dei messaggi di livello INFO nel file jsrvr.log per impostazione predefinita:

- PDMContextListener: genera una voce di registro all'avvio e all'arresto dei servizi.
- PDMweb: genera una voce di registro per le operazioni eseguite sull'interfaccia utente.
- UploadServlet: genera una voce di registro quando uno o più file vengono allegati a un ticket.
- pdmExport: genera una voce di registro quando l'opzione Esporta viene selezionata nei moduli di elenco.
- pdm_report: genera una voce di registro quando il menu Report viene selezionato nei moduli di elenco.
- page_cache: genera una voce di registro per le operazioni eseguite sull'interfaccia utente.
- ProcessServlet: genera una voce di registro durante l'installazione di CA Workflow e l'accesso alle attività di CA Workflow.

  Nota: anche i daemon pdm_rpc generano una voce di registro per queste azioni.
- BOServlet: genera una voce di registro quando si configura CA Business Intelligence e la scheda Report viene selezionata.

Interfaccia PDA

CA SDM supporta la terminologia ITIL per l'interfaccia Personal Digital Assistant (PDA). Questa interfaccia consente agli utenti finali di creare Richieste, Incidenti e Problemi e di cercare i seguenti tipi di ticket:

- Incidenti
- Problemi
- Richieste
- Ordini di cambiamento
- Issue

Gli analisti possono utilizzare l'interfaccia PDA. L'interfaccia si adatta al ruolo specificato nel campo*Ruolo PDA* del tipo di accesso del contatto.

L'interfaccia PDA viene visualizzata su tutti i dispositivi e i browser non supportati.

Il servizio di ricerca di un contatto funziona unicamente sui browser PDA che supportano schede e finestre del browser multiple. Il funzionamento della funzionalità di multi-tenancy è simile a quello dell'interfaccia del browser, tuttavia non consente di visualizzare l'elenco a discesa per la selezione multi-tenancy. Quando si crea il ticket, la proprietà viene basata sul richiedente, sull'utente finale interessato e sull'analista.

Il calcolo automatico della priorità (APC) consente di definire la priorità durante la creazione dell'Incidente/Problema, in base agli attributi, l'urgenza, l'impatto, l'area Richiesta e l'utente finale interessato.

Nota: l'asterisco indica un campo obbligatorio. Ad esempio, quando si crea una Richiesta è necessario specificare l'utente finale interessato e la priorità. L'Interfaccia PDA non supporta allegati durante la creazione del ticket.

Registrazione REST

REST utilizza i pacchetti pdm_rest_util.jar e rest-core.jar contenenti il file di supporto per la registrazione log4j. Questi componenti *non* eseguono la scrittura di alcun messaggio nei registri standard (stdlog.*), ma utilizzando il componente log4j. Per impostazione predefinita, tali pacchetti registrano i messaggi di tipo INFO, ERROR e WARN. I pacchetti Java utilizzano lo stesso file delle proprietà di configurazione log4j, pertanto ciascun pacchetto registra i messaggi nello stesso file di output. Il file *rest.log4j.properties* è disponibile nella directory $NX_ROOT\site\cfg\.

Per aumentare il livello di registro a livello TRACE o DEBUG, aggiornare la sezione seguente nel file *rest.log4j.properties:*

```
log4j.rootCategory=debug, jrestlog
```

Individuare il file di output, come definito nel file delle proprietà di configurazione disponibile nella directory seguente:

```
$NX_ROOT\log\jrest.log
```

Abilitazione della registrazione CXF

USDK> disabilita la registrazione CXF per impostazione predefinita in quanto può influire sulle prestazioni dell'ambiente di produzione. Se l'ambiente in uso richiede la registrazione ai fini di debug, l'amministratore può modificare il file beans.xml per abilitare la registrazione CXF.

Procedere come descritto di seguito:

1. Individuare il file beans.xml nella directory seguente:

   ```
   NX_ROOT\bopcfg\www\CATALINA_BASE_REST\webapps\caisd-rest\WEB-INF
   ```

2. Individuare la sezione seguente del file XML:

   ```
   <cxf:bus>
       <cxf:features>
       </cxf:features>
   </cxf:bus>
   ```

3. Aggiungere <cxf:logging/> alla sezione, come mostrato nell'esempio seguente:

   ```
   <cxf:bus>
       <cxf:features>
          <cxf:logging/>
       </cxf:features>
   </cxf:bus>
   ```

4. Salvare il file XML.

Configurazione ITIL

La norma *ITIL (Information Technology Infrastructure Library)* è una raccolta di procedure ottimali per la gestione dei data center informatici. Oltre a definire i processi consigliati, uno dei principali vantaggi offerti da ITIL è la definizione precisa della terminologia comune utilizzata nell'ambito del data center. Spesso nel mondo IT, la stessa parola viene utilizzata con significati diversi, oppure persone diverse utilizzano una determinata parola con accezioni differenti. ITIL consente di ridurre questo problema.

Sono disponibili i seguenti tipi di ticket:

- Richiesta
- Ordine di cambiamento
- Issue
- Incidente
- Problema

Importante. CA SDM supporta solo un'interfaccia ITIL. L'interfaccia ITIL supporta gli oggetti dati non utilizzati nelle versioni non ITIL precedenti del prodotto, quali i ticket Problema e Incidente.

ITIL offre le seguenti funzionalità:

- Genera un'interfaccia ITIL per l'installazione di CA SDM.
- Consente di variare il database, i moduli e i campi CA SDM rispetto a un'installazione standard e di conformarli invece alle convenzioni ITIL.

  Importante. Quando si esegue l'aggiornamento di un sistema esistente, deselezionare la casella di controllo "Carica dati predefiniti" per mantenere le tabelle e i dati del database. In caso contrario, tutti i dati esistenti vanno persi. Per ulteriori informazioni sulla migrazione da un ambiente non-ITIL, consultare la *Guida all'implementazione*.

Discipline dei servizi ITIL

ITIL descrive le procedure ottimali per diverse discipline. Le discipline descritte in Service Support e Service Delivery forniscono tutti gli strumenti necessari per la corretta gestione dei servizi di un'organizzazione. Le dieci discipline di gestione dei servizi sono strettamente correlate al fine di creare un'infrastruttura IT di alto livello per le aziende.

Il supporto dei servizi include le seguenti discipline:

- Gestione degli incidenti
- Gestione dei problemi
- Gestione dei Cambiamenti
- Gestione versione
- Gestione della configurazione

CA SDM si occupa in modo particolare di Gestione incidenti, Gestione problemi, Gestione cambiamenti e Gestione configurazione.

In Erogazione dei servizi sono incluse le seguenti discipline:

- Service Management
- Gestione disponibilità
- Gestione capacità
- Gestione finanziaria per i servizi IT
- Gestione continuità servizi IT

CA SDM è destinato in modo specifico alla gestione dei servizi.

Opzioni delle interfacce per i dipendenti e per gli utenti Guest

È possibile utilizzare CA SDM per configurare interfacce separate per i dipendenti e gli utenti Guest. La configurazione di interfacce separate può essere eseguita utilizzando Gestione opzioni nella scheda Amministrazione. Tali interfacce sono controllate dai seguenti valori:

employee_intf_incident_support

Vengono visualizzati i seguenti valori:

- Solo richiesta
- Solo incidente
- Sia Incidente che Richiesta

guest_intf_incident_support

Vengono visualizzati i seguenti valori:

- Solo richiesta
- Solo incidente
- Sia Incidente che Richiesta

Importante. Se si tratta di una nuova installazione, ITIL viene configurato per impostazione predefinita con il valore *Solo Incidente*. Se si esegue la migrazione da una configurazione non ITIL precedente, vengono installate le opzioni, ma i valori vengono impostati su *Solo Richiesta*.

Configurazione dell'interfaccia per i dipendenti

È possibile configurare l'interfaccia per i dipendenti per visualizzare incidenti, richieste o entrambi.

Per configurare l'interfaccia per i dipendenti

1. Fare clic sulla scheda Amministrazione.

   Viene visualizzata la console di amministrazione.

2. Fare clic su Gestione Opzioni, Gestione Richiesta.

   Viene visualizzato l'Elenco opzioni.

3. Fare clic su employee_intf_incident_support.

   Viene visualizzata la pagina Dettagli opzioni.

4. Impostare uno dei seguenti valori per il campo Valore opzione:

   Solo Incidente

   (Impostazione ITIL predefinita) Consente di visualizzare solo i tipi di ticket incidente nell'interfaccia per i dipendenti.

Solo Richiesta

Consente di visualizzare solo i tipi di ticket richiesta nell'interfaccia per i dipendenti.

Sia Incidente che Richiesta

Consente di visualizzare sia i tipi di ticket incidente che richiesta nell'interfaccia per i dipendenti.

Fare clic su Salva.

5. Fare clic su Aggiorna per confermare le selezioni.

   La pagina Dettagli opzioni viene aggiornata.

6. Chiudere la pagina Dettagli opzioni.

   Viene visualizzato l'Elenco opzioni.

Configurazione dell'interfaccia per gli utenti Guest

È possibile configurare l'interfaccia per gli utenti Guest per visualizzare incidenti, richieste o entrambi.

Per configurare l'interfaccia per gli utenti Guest

1. Fare clic sulla scheda Amministrazione.

   Viene visualizzata la console di amministrazione.

2. Fare clic su Gestione Opzioni, Gestione Richiesta.

   Viene visualizzato l'Elenco opzioni.

3. Fare clic su guest_intf_incident_support.

   Viene visualizzata la pagina Dettagli opzioni.

4. Impostare uno dei seguenti valori per il campo Valore opzione:

   Solo Incidente

   (Impostazione predefinita) Consente di visualizzare solo i tipi di ticket incidente nell'interfaccia per gli utenti Guest.

   Solo Richiesta

   Consente di visualizzare solo i tipi di ticket richiesta nell'interfaccia per gli utenti Guest.

   Sia Incidente che Richiesta

   Consente di visualizzare sia i tipi di ticket incidente che richiesta nell'interfaccia per gli utenti Guest.

   Fare clic su Salva.

5. Fare clic su Aggiorna per confermare le selezioni.

   La pagina Dettagli opzioni viene aggiornata.

6. Chiudere la pagina Dettagli opzioni.

   Viene visualizzato l'Elenco opzioni.

Protezione del registro attività

L'opzione di protezione del registro attività impedisce agli utenti finali l'aggiornamento dei campi di un registro attività. È possibile selezionare l'opzione interna per evitare che un cliente visualizzi il registro.

La protezione del registro attività influenza i registri attività dei seguenti tipi di ticket:

- Richiesta
- Ordine di cambiamento
- Issue
- Incidente
- Problema

Abilitazione della protezione del registro attività

È possibile abilitare la protezione del registro attività da Gestione opzioni nella scheda Amministrazione.

Per abilitare la protezione del registro attività

1. Fare clic sulla scheda Amministrazione.

   Viene visualizzata la console di amministrazione.

2. Fare clic su Gestione opzioni, Richiesta-Cambiamento-Issue.

   Viene visualizzato l'Elenco opzioni.

3. Fare clic su activity_log_security.

   Viene visualizzata la pagina Dettagli opzioni.

4. Fare clic su Modifica e selezionare uno dei seguenti valori delle opzioni:

   Modificabile

   (Predefinito) Consente di modificare tutti i campi del registro attività mediante l'interfaccia o i servizi Web.

Protetto da scrittura

Visualizza il registro attività in sola lettura. Se si seleziona l'opzione interna, il registro può essere modificato solo dagli utenti interni e non può essere visualizzato dal cliente.

Nota: se è abilitata l'opzione di protezione, viene visualizzato un messaggio di errore che indica che il registro attività è di sola lettura se si tenta di modificarlo tramite l'interfaccia Web oppure origini esterne come i servizi Web.

Fare clic su Salva.

5. Fare clic su Aggiorna per confermare le selezioni. Chiudere la finestra.

   Viene abilitata la protezione del registro attività.

Importante. Non è possibile disinstallare l'opzione activity_log_security. È solo possibile modificare il valore dell'opzione in Modificabile o Protetto da scrittura in Gestione opzioni, Richiesta-Cambiamento-Issue.

Impatto su Web Screen Painter

La funzione di protezione del registro attività $NX_ACTIVITY_LOG_ SECURITY include i seguenti attributi (time_spent, time_stamp e description) per oggetti alg, chgalg e issalg in Majic.

Esempio: $NX_ACTIVITY_LOG_SECURITY per l'algoritmo dell'oggetto in cm.maj

In questo esempio, $NX_ACTIVITY_LOG_SECURITY viene visualizzato in tre attributi per l'algoritmo dell'oggetto in cm.maj:

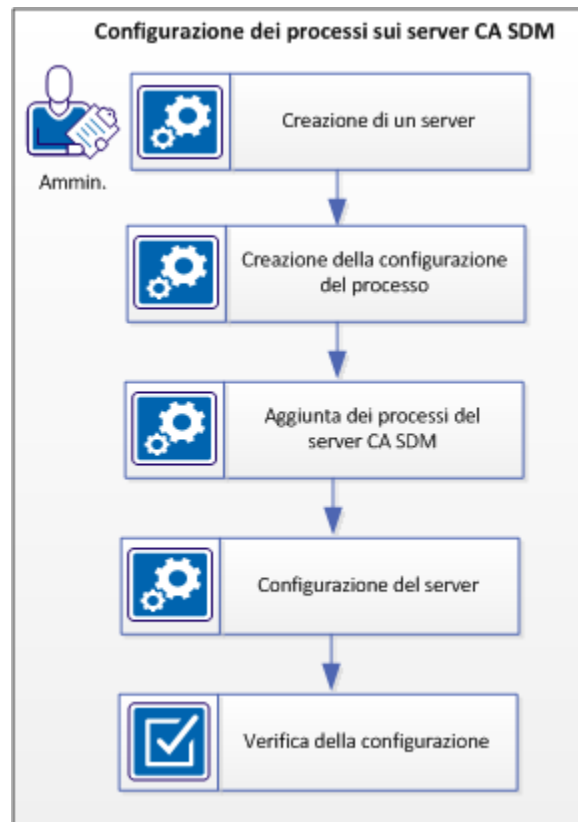
```
time_spent DURATION $NX_ACTIVITY_LOG_SECURITY {ON_POST_VAL update_cr_timespent(
call_req_id ) 50 ;
 } ;
time_stamp DATE $NX_ACTIVITY_LOG_SECURITYÂ Â Â { ON_NEW DEFAULT NOW ; } ;
descriptionÂ Â Â Â  STRING Â Â Â $NX_ACTIVITY_LOG_SECURITY;
```

In Web Screen Painter il campo *Aggiornabile solo per nuovo record* viene disattivato quando il valore della parola chiave restituisce un valore WRITE_NEW.

Nota: per informazioni sul database Web Screen Painter, consultare la *Guida all'implementazione*.

Configurazione dei processi per i server di CA SDM

L'amministratore può aggiungere o modificare i processi e i daemon per migliorare le prestazioni dei server di CA SDM. È possibile configurare le gestioni oggetto, i motori Web, Web director e altri processi per i server CA SDM dell'ambiente in uso. È possibile aggiungere processi su più server per aumentare il volume e le prestazioni, nonché migliorare la protezione.

Il diagramma seguente mostra come configurare i processi sui server CA SDM:

Procedere come descritto di seguito:

1. Creare un server (a pagina 68).
2. Creare la configurazione di un processo (a pagina 69).
3. Aggiungere i processi server di CA SDM (a pagina 71).
4. Configurare il server. Per ulteriori informazioni su come configurare il server, consultare lo scenario *Configurazione dei server di CA SDM* o la *Guida all'implementazione*.
5. Verificare la configurazione (a pagina 84).

Aggiunta di un server

Se non si dispone di alcun server esistente, aggiungere i record per tutti i server che si desidera installare nella propria distribuzione di CA SDM.

Procedere come descritto di seguito:

1. Accedere al server seguente, a seconda della configurazione di CA SDM:
   - Convenzionale: server primario
   - Disponibilità avanzata: server in background
2. Selezionare Sistema, Server dalla scheda Amministrazione.

   Viene visualizzata la pagina Elenco server.
3. Fare clic su Crea nuovo per aggiungere un record per il server seguente, a seconda della configurazione di CA SDM:
   - Convenzionale: server secondario
   - Disponibilità avanzata: server applicazioni o server di standby

   Viene visualizzata la pagina Crea Nuovo server.
4. Completare i campi del server per il server secondo necessità.
5. Fare clic su Salva.

   I dettagli del server sono stati aggiunti.

Creazione di campi del server

Durante la creazione di un server vengono visualizzati i seguenti campi:

Nome host

Specifica il nome host locale del server. Il nome host locale è archiviato nella tabella usp_servers nella colonna di local_host.

Importante. Accertarsi che il nome host sia stato immesso con la distinzione tra maiuscole e minuscole nella tabella usp_server.

Fuso orario

Consente di specificare il fuso orario del luogo in cui si trova il server. Il fuso orario viene utilizzato per attivare eventi nel sistema se l'opzione Use End User Time Zone (Usa fuso orario utente finale) non è stata selezionata o se non è stato specificato alcun fuso orario per il tipo di servizio.

Stato record

Indica lo stato del server. Lo stato attivo indica che il server è incluso nella distribuzione di CA SDM.

Importante. Se un server è stato disattivato, si consiglia di non avviare i servizi di CA SDM su tale server. Questa azione può provocare una comportamento imprevisto.

Tipo di server

Specifica il tipo di server che si desidera configurare. È possibile selezionare i tipi di server seguenti, a seconda della propria configurazione di CA SDM:

- Disponibilità avanzata: server applicazioni o server di standby
- Convenzionale: server secondario

Configurato

Questo campo è disponibile solo per la configurazione con disponibilità avanzata. Indica lo stato del server configurato. Il valore predefinito di questo campo è No. Il valore viene aggiornato a Sì dopo aver eseguito correttamente pdm_configure su tale server. In caso di modifica di uno dei valori del campo immessi automaticamente di un record del server, il campo Configurato viene impostato su No.

Creazione della configurazione di un processo

È possibile creare una configurazione di processo per l'installazione di CA SDM o modificarne una esistente in base ai propri requisiti.

Considerare i punti seguenti durante la configurazione di un processo:

- Nella configurazione convenzionale, si crea la configurazione solo per un server primario e non per i server secondari. È necessario includere tutti i dettagli di configurazione dei server secondari all'interno della configurazione creata per il server primario. Ad esempio, per aggiungere un motore Web con i dettagli del nome host dei server secondari, aprire la configurazione per il server primario e aggiungere i dettagli necessari.
- Per il tipo di configurazione con disponibilità avanzata, è possibile creare configurazioni solo per il server specifico. Accertarsi di aver creato la stessa configurazione per il server in background e il server di standby.

Procedere come descritto di seguito:

1. Selezionare Sistemi, Configurazioni nella scheda Amministrazione.

   Viene visualizzata la pagina Elenco configurazioni.

2. Fare clic su Crea Nuovo per aggiungere una configurazione server.

   Viene visualizzata la pagina Crea Nuova configurazione.

3. Inserire i dati nei seguenti campi:

   Importante. Utilizzare unicamente caratteri dell'alfabeto inglese per tutti i campi di immissione, in tutte le lingue localizzate.

   Nome configurazione

   Specifica il nome che si desidera assegnare alla configurazione creata.

   Disponibilità avanzata

   Indica se la configurazione creata rientra nel tipo convenzionale o nel tipo con disponibilità avanzata. Selezionare Sì se la configurazione è valida per il tipo di configurazione con disponibilità avanzata.

   Nota: Non è possibile implementare le configurazioni create per un tipo di configurazione (disponibilità avanzata o convenzionale) per l'altro tipo.

   Nome host

   Specifica il nome host per la configurazione. Il nome host viene preso dai record di server configurati nella pagina Server. È possibile fare clic sul pulsante Cerca per la ricerca dei server aggiunti all'installazione di CA SDM.

   Stato record

   Specifica se il record di configurazione server è attivo.

   Configurazione corrente

   Indica che la configurazione viene applicata sul server di CA SDM selezionato. Questo campo è di sola lettura e viene aggiornato in base alla configurazione selezionata mentre si esegue l'utilità di configurazione server (pdm_configure).

4. Fare clic su Salva.

   La configurazione viene salvata. Nuove schede vengono abilitate nella pagina per aggiungere gestioni oggetti, motori Web, Web Director e altri processi.

   Nota: Una volta salvata la configurazione, i campi relativi al nome host e alla disponibilità avanzata diventano di sola lettura.

   Fare clic su Modifica in elenco nella pagina di Elenco configurazioni per modificare lo stato record della configurazione di un processo.

   Nota: non è possibile modificare lo stato record se la configurazione attuale di un server selezionato è in uso.

Aggiunta dei processi al server di CA SDM

È possibile configurare le gestioni oggetto, i motori Web, Web director e altri processi per i server CA SDM dell'ambiente in uso. Si consiglia di acquisire dimestichezza con le informazioni seguenti prima di configurare i processi di CA SDM:

Importante: Riconfigurare il server specifico tramite l'esecuzione dell'utilità pdm_configure sul server una volta aggiunti i processi di CA SDM.

Gestioni oggetto

Le gestioni oggetto consentono di gestire tutti gli oggetti di CA SDM. Ciascuna gestione oggetto dispone di un nome associato utilizzato per la comunicazione con altri oggetti. I sistemi Enterprise con server multiprocessore possono aggiungere gestioni oggetto per distribuire il carico di elaborazione. In base al tipo di configurazione in uso, CA SDM esegue l'installazione di una gestione oggetto predefinita sui seguenti server:

- Convenzionale: server primario
- Disponibilità avanzata: tutti i server

Nota: Non è possibile modificare la gestione oggetto predefinita, ma è possibile aggiungere altre gestioni oggetto a qualsiasi server.

Motori Web

I motori Web preparano le pagine Web per il client Web. Tutti i sistemi dispongono di uno o più motori Web. Ciascun motore Web esegue la connessione a una gestione oggetto per elaborare tutte le richieste relative agli oggetti di CA SDM. Ogni motore Web può essere eseguito e vi si può accedere direttamente. Nell'accesso diretto, ogni browser Web visualizza l'interfaccia CGI specifica per un determinato motore Web. Con questo approccio, tutti i client possono connettersi a un motore Web e sovraccaricarlo, mentre gli altri motori Web restano inutilizzati. Per gestire questo traffico intenso, è possibile assegnare due o più moduli Web a un Web Director singolo. Tutte le richieste indirizzate ai motori Web vengono destinate al Web Director. Il Web Director reindirizza così il client al motore Web con maggiore disponibilità.

In base al tipo di configurazione in uso, CA SDM esegue l'installazione di un motore Web predefinito sui seguenti server:

- Convenzionale: server primario
- Disponibilità avanzata: tutti i server

Web Director

I Web Director sono facoltativi e vengono utilizzati quando due o più moduli Web sono installati su un server singolo. Web Director riceve le richieste di connessione dagli utenti, seleziona un motore Web per gestire la richiesta e reindirizza la richiesta a tale motore. Il processo risulta trasparente per l'utente finale che accede a CA SDM sempre con lo stesso URL, indipendentemente dal numero di moduli Web configurati. È possibile utilizzare i Web Director per gli scopi seguenti:

- Per configurare CA SDM per l'uso del protocollo SSL.

  Il protocollo HTTPS consente la crittografia delle transazioni Web, garantendo la massima protezione dei dati personali, in particolar modo delle password. Tuttavia, le pagine che utilizzano il protocollo SSL non sono idonee all'uso della cache del browser, poiché potrebbe avere un impatto negativo sulle prestazioni.

- Per indirizzare gli accessi a uno o più motori Web specifici.

  Dopo l'autenticazione dell'utente, Web Director può spostare la sessione su un altro motore Web, che può trovarsi su un server HTTP differente. Questa impostazione consente di configurare il protocollo SSL per un motore Web, così da proteggere le password e utilizzare al tempo stesso il protocollo HTTP per le transazioni.

- Per utilizzare più Web Director al fine di gestire più gruppi di motori Web

  Questa configurazione può essere utile per le organizzazioni che si trovano in aree geografiche differenti e che desiderano individuare i gruppi di motori Web fisicamente più vicini agli utenti finali.

Alias

Gli alias corrispondono a nomi facilmente identificabili che possono essere creati per i nomi slump della gestione oggetto. È possibile creare alias per una gestione oggetto specifica o per un gruppo di gestioni oggetto. È possibile utilizzare questi alias al posto di un nome di gestione oggetto durante la configurazione dei processi di CA SDM. In CA SDM, l'utilizzo degli alias è facoltativo.

Daemon della conoscenza

Applicabile solo al tipo di configurazione convenzionale.

I daemon della conoscenza forniscono l'archivio della conoscenza per CA SDM (documenti della conoscenza, processo di approvazione, autorizzazioni, notifiche e così via). Per impostazione predefinita, CA SDM configura il daemon della conoscenza sul server primario. È possibile spostare il daemon in un server secondario modificando il nome host.

Autenticazione degli utenti connessi

Applicabile solo al tipo di configurazione convenzionale.

Per impostazione predefinita, CA SDM configura il daemon di autenticazione utente di accesso sul server primario. È possibile spostare il daemon in un server secondario modificando il nome host.

Database virtuale LDAP

Applicabile solo al tipo di configurazione convenzionale.

Per impostazione predefinita, CA SDM configura il daemon del database virtuale LDAP sul server primario. È possibile spostare il daemon in un server secondario modificando il nome host.

Daemon del repository

Applicabile solo al tipo di configurazione convenzionale.

Il daemon del repository consente di individuare i record degli allegati salvati nella directory di repository. L'interfaccia utente Web CA SDMconsente di aggiungere processi solo per i server secondari. Dopo avere aggiunto il processo mediante l'interfaccia utente Web, abilitare l'opzione corrispondente durante la configurazione di CA SDM. Per ulteriori informazioni sull'abilitazione dei processi, consultare la *Guida in linea alla configurazione del server*.

Visualizzatore

Applicabile solo al tipo di configurazione convenzionale.

È possibile configurare il visualizzatore su un server di CA SDM per l'utilizzo dei servizi Web. L'interfaccia utente Web CA SDMconsente di aggiungere processi solo per i server secondari. Dopo avere aggiunto il processo mediante l'interfaccia utente Web, abilitare l'opzione corrispondente durante la configurazione di CA SDM. Per ulteriori informazioni sull'abilitazione dei processi, consultare la *Guida in linea alla configurazione del server*.

Servizi Web REST per il server Tomcat

Applicabile solo al tipo di configurazione convenzionale.

I servizi Web REST consentono di configurare l'interfaccia utente Web affinché CA SDM sia in grado di comunicare con l'esterno. L'interfaccia utente Web CA SDMconsente di aggiungere processi solo per i server secondari. Dopo avere aggiunto il processo mediante l'interfaccia utente Web, abilitare l'opzione corrispondente durante la configurazione di CA SDM. Per ulteriori informazioni sull'abilitazione dei processi, consultare la *Guida in linea alla configurazione del server*.

Support Automation

Applicabile solo al tipo di configurazione convenzionale.

L'interfaccia utente Web CA SDMconsente di aggiungere processi solo per i server secondari. Dopo aver aggiunto il processo tramite l'interfaccia utente Web, abilitare l'opzione specifica durante la configurazione di CA SDM. Per ulteriori informazioni sull'abilitazione dei processi, consultare la *Guida in linea alla configurazione del server*. È possibile aggiungere un solo processo di Support Automation per ciascun server secondario. È possibile configurare i seguenti server di Support Automation:

Server principale SA

Specifica il server su cui è installato Support Automation (SA). È possibile aggiungere il server principale SA solo a un server secondario.

Server gestione oggetti SA dedicato

Il server su cui si trova la gestione oggetto per la configurazione di Support Automation. È possibile configurare il server della gestione oggetto dedicato su un server secondario.

Nota: È possibile aggiungere un server di gestione oggetto dedicato solo se è configurato il server principale SA.

Server di routing dei messaggi SA

È possibile configurare il server di routing dei messaggi su un server secondario in modo da gestire più sessioni di controllo remoto e migliorare le prestazioni durante le sessioni di assistenza.

Server proxy socket SA

È possibile configurare il server proxy socket su un server secondario per eliminare il carico dal server principale durante operazioni di Support Automation, quali la crittografia/decrittografia, che richiedono un uso elevato della CPU.

Convertitore UNI

È possibile aggiungere un convertitore UNI ai server in esecuzione sulla piattaforma Unix. È possibile aggiungere il convertitore UNI ai server seguenti:

- Convenzionale: server primario, server secondario
- Disponibilità avanzata: server applicazioni

Convertitore TNG

È possibile aggiungere un convertitore TNG ai server in esecuzione sulla piattaforma Windows. È possibile aggiungere il convertitore TNG ai server seguenti:

- Convenzionale: server primario, server secondario
- Disponibilità avanzata: server applicazioni

Nota: Se il convertitore TNG è gestito con la gestione daemon, si avvia e si arresta insieme agli altri daemon. Se è necessario che il convertitore TNG acquisisca gli eventi dopo l'arresto dei daemon di CA SDM, avviare e interrompere il convertitore TNG come servizio.

Aggiunta di gestori oggetti

L'aggiunta di gestioni oggetto ai server di CA SDM migliora le prestazioni complessive del sistema. CA SDM installa una gestione oggetto predefinita su tutti i server. Non è possibile modificare la gestione oggetto predefinita, mentre è possibile aggiungere più gestioni oggetto su qualsiasi server di CA SDM per aumentare le prestazioni dei server. In base al tipo di configurazione in uso, CA SDM esegue l'installazione di una gestione oggetto predefinita sui seguenti server:

- Convenzionale: server primario.
- Disponibilità avanzata: tutti i server.

Procedere come descritto di seguito:

1. Selezionare Sistemi, Configurazioni nella scheda Amministrazione.

   Viene visualizzata la pagina Elenco configurazioni.

2. Selezionare la configurazione a cui si desidera aggiungere la gestione oggetto.

   Viene visualizzata la pagina Dettagli configurazione.

3. Selezionare la scheda Gestioni oggetto.

   Viene visualizzata la pagina Elenco Gestioni oggetto con le gestioni oggetto configurate per il server. In elenco viene mostrata anche la gestione oggetto predefinita (se presente).

4. Fare clic su Aggiungi gestione oggetto.

   Viene visualizzata la pagina Crea nuova gestione oggetto.

5. Inserire i dati nei seguenti campi:

   Importante. Utilizzare unicamente caratteri dell'alfabeto inglese per tutti i campi di immissione, in tutte le lingue localizzate.

   Nome host

   Specifica il nome host a cui si desidera aggiungere la gestione oggetto. È possibile fare clic sul pulsante Cerca per la ricerca dei server aggiunti all'installazione di CA SDM.

   Per un tipo di configurazione con disponibilità avanzata, il nome host è di sola lettura e viene compilato automaticamente in base al nome host indicato in fase di creazione della configurazione.

   Nome visualizzato

   Specifica il nome visualizzato per la gestione oggetto. Il nome visualizzato sui client indica la gestione oggetto a cui si è connessi.

   Gruppo Gestione oggetto

   Specifica il nome del gruppo a cui viene aggiunta la gestione oggetto.

   Importante. Utilizzare unicamente caratteri dell'alfabeto inglese per il nome di gruppo dell'oggetto, in tutte le lingue localizzate.

   È possibile raggruppare le gestioni oggetto in modo da assegnare gruppi per fornire i servizi a specifici gruppi di moduli Web. Gli utenti che richiedono questa funzionalità di solito dispongono di motori Web separati fisicamente dal server primario e desiderano utilizzare una gestione oggetto con il modulo Web. Gli utenti raggruppano i gestori oggetti assegnati ai motori Web locali, quindi assegnano i motori Web al gruppo di gestori oggetti.

   Maschera di accettazione

   Specifica la maschera per la gestione oggetto. La funzionalità della maschera di accettazione indica alla gestione oggetto i client da cui accettare le connessioni.

   Ad esempio, un motore Web tenta di collegarsi a una gestione oggetto chiamata web:seattle:1, web:seattle:2 o web:texas:1. È possibile specificare una maschera di accettazione di tipo web:seattle.* per accettare tutte le connessioni da Seattle e rifiutare le altre. È possibile anche specificare una maschera di tipo web:.* per accettare le connessioni dai moduli Web e rifiutare le connessioni dai client.

Stato record

Specifica se la gestione oggetto è attiva o non attiva.

Nota: Prima di impostare lo stato del record per una gestione oggetto su Non attivo, è necessario rimuovere il collegamento tra la gestione oggetto e i moduli Web associati.

6. Fare clic su Salva.

   La gestione oggetto aggiunta viene visualizzata nell'elenco delle gestioni oggetto.

Aggiunta di motori Web o Web Director

I motori Web si connettono a una gestione oggetto per elaborare tutte le richieste relative agli oggetti di CA SDM. I Web Director sono facoltativi e vengono utilizzati quando due o più moduli Web sono installati su un server singolo. È possibile configurare Web Director su qualsiasi server. A seconda della configurazione di CA SDM, CA SDM installa un motore Web predefinito sui server seguenti:

- Convenzionale: server primario.
- Disponibilità avanzata: tutti i server.

Procedere come descritto di seguito:

1. Selezionare Sistemi, Configurazioni nella scheda Amministrazione.

   Viene visualizzata la pagina Elenco configurazioni.

2. Selezionare la configurazione a cui si desidera aggiungere il motore Web o il Web Director.

   Viene visualizzata la pagina Dettagli configurazione.

   Nota: se si cambia la configurazione per la prima volta, creare innanzitutto una configurazione. Quando si desidera cambiare una configurazione, creare o copiarne sempre una esistente. Questo processo consente di ritornare alla configurazione precedente, se necessario.

3. Selezionare la scheda Motori Web/Web Director.

   Viene visualizzata la pagina Elenco Motori Web/Web Director con i motori Web e i Web Director configurati per il server.

   - Convenzionale: per impostazione predefinita esiste un motore Web sul server primario. È possibile aggiungere Web Director a qualsiasi server.
   - Disponibilità avanzata: per impostazione predefinita esiste un motore Web su tutti i server. È possibile aggiungere più Web Director su qualsiasi server di CA SDM.

4. Fare clic su Aggiungi motore Web/Web Director.

   Viene visualizzata la pagina Crea nuovo motore Web/Web Director.

5. Inserire i dati nei seguenti campi:

   Importante. Utilizzare unicamente caratteri dell'alfabeto inglese per tutti i campi di immissione, in tutte le lingue localizzate.

   Nome host

   Specifica il nome host per il motore Web o il Web Director. È possibile fare clic su Cerca per cercare i server.

   Per un tipo di configurazione con disponibilità avanzata, il nome host è di sola lettura e viene compilato automaticamente in base al nome host indicato in fase di creazione della configurazione.

   Tipo

   Specifica se configurare un motore Web o il Web Director. In base all'opzione selezionata, i relativi campi vengono compilati automaticamente.

   - Selezionare Motore Web se si desidera configurare un motore Web.
   - Selezionare Web Director se si desidera configurare un Web Director.

   Nota: Verificare di aver selezionato l'opzione appropriata. Una volta salvata la configurazione, non è possibile modificare il tipo di processo.

   Web Director

   Specifica il Web Director assegnato al motore Web. È possibile fare clic su Cerca per cercare i Web Director aggiunti al server.

   Nota: In caso di implementazione di uno schema di bilanciamento del carico del motore Web e/o di accesso SSL, è necessario assegnare almeno due motori Web allo stesso Web Director.

   Nome CGI

   Specifica il nome CGI univoco per il motore Web. Corrisponde al nome di un eseguibile CGI quando IIS o Apache vengono utilizzati come server HTTP, mentre è un parametro servlet quando Tomcat viene utilizzato come server HTTP.

   Esempi: (motori Web) pdmweb1, pdmweb2, (Web Director) pdmweb_d1 e pdmweb_d2.

   Impostazione predefinita: pdmweb.exe (il nome CGI deve essere univoco).

Numero porta di CGI

Specifica la porta per la comunicazione dei client Web di CA SDM. Il numero di porta CGI è lo stesso della porta su cui è in esecuzione il server Tomcat.

Impostazione predefinita: 8080

Protocollo

Specifica il protocollo per accedere al motore Web.

- Selezionare HTTPS se il motore Web è configurato per la gestione di tutte le richieste di autenticazione utente per client Web di CA SDM.
- Selezionare HTTP se il motore Web è configurato per la gestione di tutte le richieste di autenticazione non utente per client Web (una volta autenticato l'utente con il motore Web di accesso protetto).

Stato record

Specifica se il motore Web o il Web Director è attivo o non attivo.

Nota: Prima di impostare lo stato del record di un Web Director su Non attivo, rimuovere il collegamento tra il Web Director e i motori Web associati.

Gestioni oggetto

Specifica la gestione oggetto che si desidera assegnare al motore Web.

Valore predefinito

Specifica che la gestione oggetto predefinita è assegnata al motore Web.

QUALSIASI

Specifica che è possibile connettere il motore Web alla gestione oggetto con maggiore disponibilità. Il valore di disponibilità indica la disponibilità del server ad accettare nuovi client. Se il valore di disponibilità è 0, significa che il motore Web non accetta alcuna sessione.

Scegli

Consente di specificare una gestione oggetto per il motore Web. Se selezionata, questa opzione consente di aggiungere più gestioni oggetto o alias alla configurazione.

6. Fare clic su Salva.

   Il motore Web o il Web Director aggiunto viene visualizzato in Elenco Motori Web/Web Director.

Aggiunta di alias

In CA SDM, l'utilizzo degli alias è facoltativo. È possibile creare alias per una gestione oggetto specifica o per un gruppo di gestioni oggetto. Prima di creare gli alias, effettuare le seguenti attività:

- Definire i gestori oggetti e aggiungerne alcuni ai gruppi.

  Ad esempio, domsrvr:group1:11, domsrvr:seattle:12, domsrvr:seattle:13, domsrvr:Tacoma:11.

- Immettere un'espressione regolare che corrisponde un gruppo di gestori oggetti.

  Ad esempio, si desidera che i client Java di Washington eseguano la connessione alla gestione oggetto di Seattle. Questi client devono connettersi a /domsrvr:seattle.*. In alternativa, è possibile definire un alias denominato SEATTLE e assegnare a tale alias il valore /domsrvr:seattle.*.

- Definire i motori Web e assegnare gli alias a tali motori.

Importante. Se sono stati creati alias per un gruppo di gestioni oggetto, verificare di aver modificato gli alias rispettivi dopo la modifica del gruppo di gestioni oggetto.

Procedere come descritto di seguito:

1. Selezionare Sistemi, Configurazioni nella scheda Amministrazione.

   Viene visualizzata la pagina Elenco configurazioni.

2. Selezionare la configurazione a cui si desidera aggiungere l'alias.

   Viene visualizzata la pagina Dettagli configurazione.

3. Selezionare la scheda Alias.

   Viene visualizzata la pagina Elenco alias con gli alias creati per il server.

4. Fare clic su Aggiungi alias.

   Viene visualizzata la pagina Crea Nuovi alias.

5. Inserire i dati nei seguenti campi:

   Importante. Utilizzare unicamente caratteri dell'alfabeto inglese per tutti i campi di immissione, in tutte le lingue localizzate.

   Nome

   Specifica il nome per l'alias creato.

   Definizione

   Specifica l'espressione regolare associata all'alias. Il formato seguente viene utilizzato per una definizione di alias:
   `domsrvr:[<group>:][<host_id><id>][.*]`

   Impostazione predefinita: /domsrvr:.*

Stato record

Specifica se l'alias è attivo o non attivo.

6. Fare clic su Salva.

   L'alias aggiunto viene visualizzato in Elenco alias.

Aggiunta di ulteriori processi

CA SDM consente di configurare i server di Support Automation, Visualizer, LDAP, KT, TNG/UNI, i daemon del repository BopLogin e il processo dei servizi Web REST per un server.

Procedere come descritto di seguito:

1. Selezionare Sistemi, Configurazioni nella scheda Amministrazione.

   Viene visualizzata la pagina Elenco configurazioni.

2. Selezionare la configurazione a cui si desidera aggiungere altri processi.

   Viene visualizzata la pagina Dettagli configurazione.

3. Selezionare la scheda Processi aggiuntivi.

   L'Elenco processi aggiuntivi visualizza l'elenco dei processi configurati per il server insieme ai processi predefiniti, se presenti.

4. Fare clic su Aggiungi processo.

   Viene visualizzata la pagina Crea nuovo processo.

5. Completare i campi seguenti in modo appropriato:

   Importante. Utilizzare unicamente caratteri dell'alfabeto inglese per tutti i campi di immissione, in tutte le lingue localizzate.

   Processo

   Indica il processo del server di CA SDM che si desidera aggiungere.

   Repository Daemon (Daemon repository)

   Applicabile solo al tipo di configurazione convenzionale.

   Specifica il daemon del repository configurato per il server. I daemon del repository supportano i repository degli allegati. Per impostazione predefinita, CA SDM configura un daemon del repository sul server primario. È possibile spostare il daemon in un server secondario modificando il nome host.

Server principale SA

Applicabile solo al tipo di configurazione convenzionale.

Specifica il server principale SA configurato per il server. È possibile configurare solo un server principale SA.

Server oggetti SA dedicato

Applicabile solo al tipo di configurazione convenzionale.

Specifica la gestione oggetto dedicata per la configurazione di Support Automation. È possibile specificare solo un server oggetti dedicato sul server primario o su quello secondario.

Nota: È possibile aggiungere un server di gestione oggetto dedicato solo se è configurato il server principale SA.

Server di routing dei messaggi SA

Applicabile solo al tipo di configurazione convenzionale.

Specifica il server di routing dei messaggi configurato per il server. È possibile configurare il server di routing dei messaggi su un server secondario in modo da gestire più sessioni di controllo remoto e migliorare le prestazioni durante le sessioni di assistenza.

Server proxy socket SA

Applicabile solo al tipo di configurazione convenzionale.

Specifica il server proxy socket configurato per il server. È possibile configurare il server proxy socket su un server secondario per eliminare il carico dal server principale durante operazioni, quali la crittografia/decrittografia, che richiedono un uso elevato della CPU.

Servizi Web REST per il server Tomcat

Applicabile solo al tipo di configurazione convenzionale.

Specifica i servizi Web REST configurati per il server. I servizi Web REST consentono di configurare l'interfaccia utente Web affinché CA SDM sia in grado di comunicare con l'esterno. L'interfaccia utente Web CA SDMconsente di aggiungere processi solo per i server secondari. Dopo avere aggiunto il processo mediante l'interfaccia utente Web, abilitare l'opzione corrispondente durante la configurazione di CA SDM. Per ulteriori informazioni sull'abilitazione dei processi, consultare la *Guida in linea alla configurazione del server*.

Convertitore TNG

È possibile aggiungere un convertitore TNG ai server in esecuzione sulla piattaforma Windows. È possibile aggiungere il convertitore TNG ai server seguenti:

Convenzionale: server primario, server secondario.

Disponibilità avanzata: server applicazioni.

Nota: Se il convertitore TNG è gestito con la gestione daemon, viene avviato e arrestato insieme agli altri daemon. Se si desidera che il convertitore TNG acquisisca gli eventi dopo l'arresto dei daemon di CA SDM, avviare e interrompere il servizio del convertitore TNG.

Convertitore UNI

Specifica il convertitore UNI configurato per rispondere a eventi UNIX. È possibile filtrare questi eventi e configurarli per la creazione di ticket e attivare altro lavoro in Service Desk. È possibile aggiungere un convertitore UNI ai server in esecuzione sulla piattaforma Unix. È possibile aggiungere il convertitore UNI ai server seguenti:

Convenzionale: server primario, server secondario.

Disponibilità avanzata: server applicazioni.

Visualizer Tomcat Server (Server Tomcat Visualizer)

Applicabile solo al tipo di configurazione convenzionale.

Specifica il visualizzatore configurato per il server.

È possibile configurare il visualizzatore su un server di CA SDM per l'utilizzo dei servizi Web. L'interfaccia utente Web CA SDMconsente di aggiungere processi solo per i server secondari. Dopo avere aggiunto il processo mediante l'interfaccia utente Web, abilitare l'opzione corrispondente durante la configurazione di CA SDM. Per ulteriori informazioni sull'abilitazione dei processi, consultare la *Guida in linea alla configurazione del server*.

Nota: È possibile configurare solo un server di Tomcat Visualizer su un server secondario.

Nome host

Specifica il server che ospita il processo aggiunto. È possibile fare clic sul pulsante Cerca per la ricerca dei server.

Stato record

Specifica se il processo aggiunto è attivo o non attivo.

6. Fare clic su Salva.

   Il processo aggiunto viene visualizzato nella pagina Elenco processi aggiuntivi.

Verifica della configurazione

- Una volta completata la configurazione e avviati i servizi correttamente, eseguire il comando pdm_status o la Gestione attività per verificare che i nuovi daemon siano stati aggiunti.
- Verificare che la configurazione corrente sia aggiornata con la configurazione selezionata durante l'operazione pdm_configure.

Capitolo 3: Interfaccia utente mobile REST di esempio

L'interfaccia utente mobile REST di esempio fornisce due interfacce utente: Analista e Dipendente. Questo esempio supporta anche i ruoli Amministratore, Analista di livello 1 e Dipendente. Dopo aver effettuato l'accesso a CA SDM, i ruoli Amministratore e Analista di livello 1 visualizzano l'interfaccia dell'analista. Il ruolo Dipendente visualizza solo l'interfaccia del dipendente. Per un accesso non valido, CA SDM respinge la richiesta di accesso e un messaggio viene visualizzato. Se un amministratore ha disattivato il calcolo automatico priorità, il campo Priorità viene visualizzato nella pagine di creazione e modifica.

Importante. Questa funzionalità è disponibile unicamente per il programma di esempio fornito con CA SDM Versione 12.9. Non si tratta di una progettazione limitata all'applicazione dei servizi Web REST.

I campi che utilizzano il suggerimento automatico richiedono una selezione del valore dal rispettivo elenco, come l'assegnatario e l'area Incidente. Se non si seleziona alcun valore, l'input dell'utente per tale campo viene cancellata.

Nota: si consiglia di eseguire la navigazione nelle interfacce REST utilizzando i pulsanti invece delle opzioni di spostamento avanti e indietro del browser. Ad esempio, selezionare Pagina iniziale o Annulla per ritornare a una pagina precedente.

Si configura REST durante la configurazione di CA SDM, ma si abilita l'interfaccia mobile di esempio manualmente (a pagina 89).

Gli analisti possono eseguire le seguenti attività:

- Visualizzare gli annunci.

  Impostazione predefinita: ordinamento per data di pubblicazione.

- Visualizzare Incidenti assegnati all'Analista da CA SDM.
- Visualizzare gli Incidenti assegnati e non assegnati.
- Ordinare gli Incidenti.

  Impostazione predefinita: ordinati in base alla data di apertura.

- Cercare un Incidente
- Creare un Incidente.

- Modificare lo stato, l'urgenza e l'impatto dell'Incidenti.
- Visualizzare e aggiornare il registro delle attività con commenti oppure specificare azioni quali la ricerca o la richiamata.

  Impostazione predefinita: ordinati in base alla data attività.

I dipendenti possono effettuare le seguenti attività:

- Visualizzare gli annunci.
- Visualizzare Incidenti aperti e chiusi creati dall'utente finale.
- Ordinare gli Incidenti, ad esempio in base alla data di apertura.
- Creare un Incidente.
- Aggiornare il registro attività con un commento.
- Cercare un Incidente
- Modificare lo stato dell'Incidente da Aperto a Chiuso o da Chiuso ad Aperto.

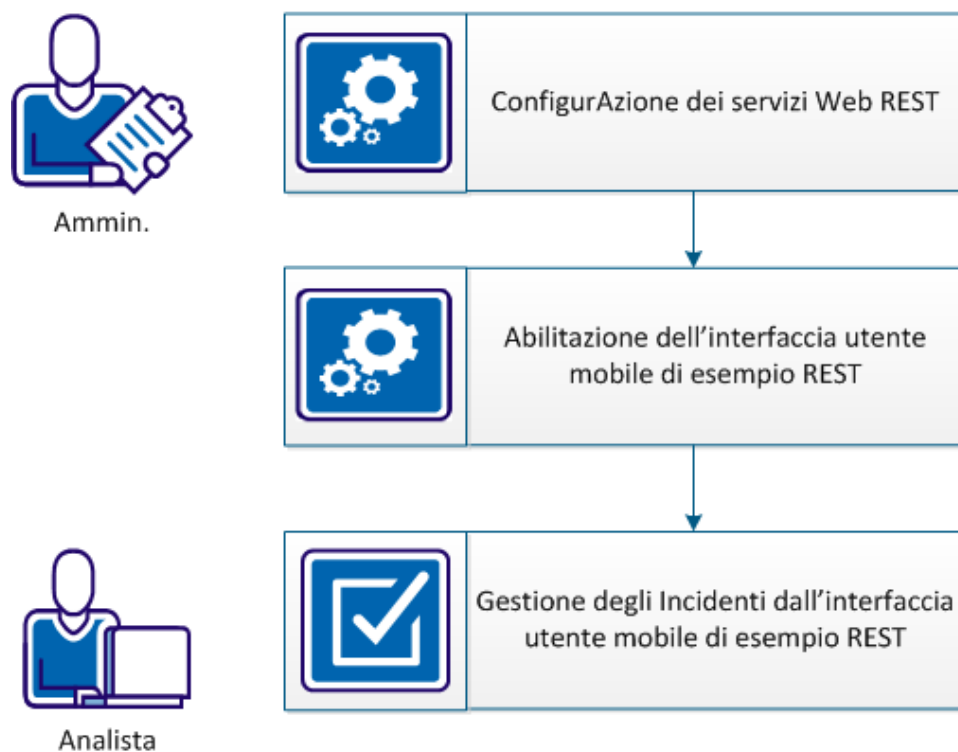
Nota: l'asterisco indica un campo obbligatorio.

Questa sezione contiene i seguenti argomenti:

Modalità di distribuzione dell'interfaccia utente mobile di esempio REST (a pagina 87)

Modalità di distribuzione dell'interfaccia utente mobile di esempio REST

L'interfaccia utente mobile di esempio REST consente agli analisti di gestire gli incidenti sui dispositivi mobili. L'amministratore abilita i servizi Web REST durante la configurazione del prodotto e copia i file nel computer CA SDM per abilitare l'interfaccia utente mobile di esempio. L'analista utilizza l'interfaccia mobile per gestire gli incidenti che gli utenti finali aprono in CA SDM.

Il diagramma seguente spiega come un amministratore abilita i servizi Web REST in modo che l'analista possa gestire gli incidenti nella coda:

Procedere come descritto di seguito:

1. Configurare i servizi Web REST (a pagina 88).
2. Abilitare l'interfaccia utente mobile di esempio REST. (a pagina 89)
3. Gestire gli incidenti dall'interfaccia mobile di esempio REST (a pagina 89).

Configurazione dei servizi Web REST

L'amministratore abilita i servizi Web REST durante la configurazione di CA SDM. Per impostazione predefinita, la configurazione di CA SDM non abilita servizi Web REST.

Procedere come descritto di seguito:

1. Completare *una* delle azioni seguenti:
   - Installare CA SDM e attendere che la finestra di dialogo di configurazione venga visualizzata.
   - Se CA SDM è già stato installato e i servizi Web REST non sono stati configurati, eseguire pdm_configure dall'interfaccia della riga di comando. In Windows, fare clic su Start, Programmi, CA, Gestione Service Desk, Configura.

   Viene visualizzata la finestra di dialogo di configurazione.
2. Confermare le informazioni di configurazione per Impostazioni generali, Account di sistema, Database e le finestre di dialogo dell'interfaccia Web.

   Verrà visualizzata la finestra di dialogo Servizi Web REST.
3. Abilitare l'opzione Configura servizi Web REST.
4. Specificare la porta Tomcat REST.

   Valore predefinito: 8050
5. Specificare la porta di arresto Tomcat REST.

   Valore predefinito: 8055
6. Fare clic su Avanti e proseguire con la configurazione di CA SDM.

   La configurazione viene completata.

Abilitazione dell'interfaccia utente mobile REST di esempio

Per impostazione predefinita, CA SDM disattiva l'interfaccia utente mobile di esempio REST per prevenire l'accesso non desiderato all'MDB. L'amministratore abilita questa interfaccia manualmente.

Procedere come descritto di seguito:

1. Individuare la directory seguente sul computer CA SDM dove i servizi Web REST sono installati e configurati:

   `$NX_ROOT/samples/sdk/rest/mobiledemo`

2. Copiare questa directory nella posizione seguente:

   `$NX_ROOT/bopcfg/www/CATALINA_BASE_REST/webapps`

   Nota: Non è necessario riavviare Tomcat.

   L'interfaccia utente mobile di esempio REST viene abilitata.

3. (Facoltativo) Se si desidera disattivare l'interfaccia utente di esempio REST, rimuovere la directory mobiledemo da /webapps.

Gestione degli incidenti dall'interfaccia mobile REST di esempio

Gli analisti o i dipendenti visualizzano l'interfaccia mobile REST di esempio sui propri dispositivi mobili per gestire gli incidenti nella coda. Ad esempio, un analista apre l'incidente 30 per registrare un commento a solo uso interno.

Procedere come descritto di seguito:

1. Aprire l'URL seguente nel proprio dispositivo mobile:

   `http://hostname:REST-Tomcat-port/mobiledemo/login.html`

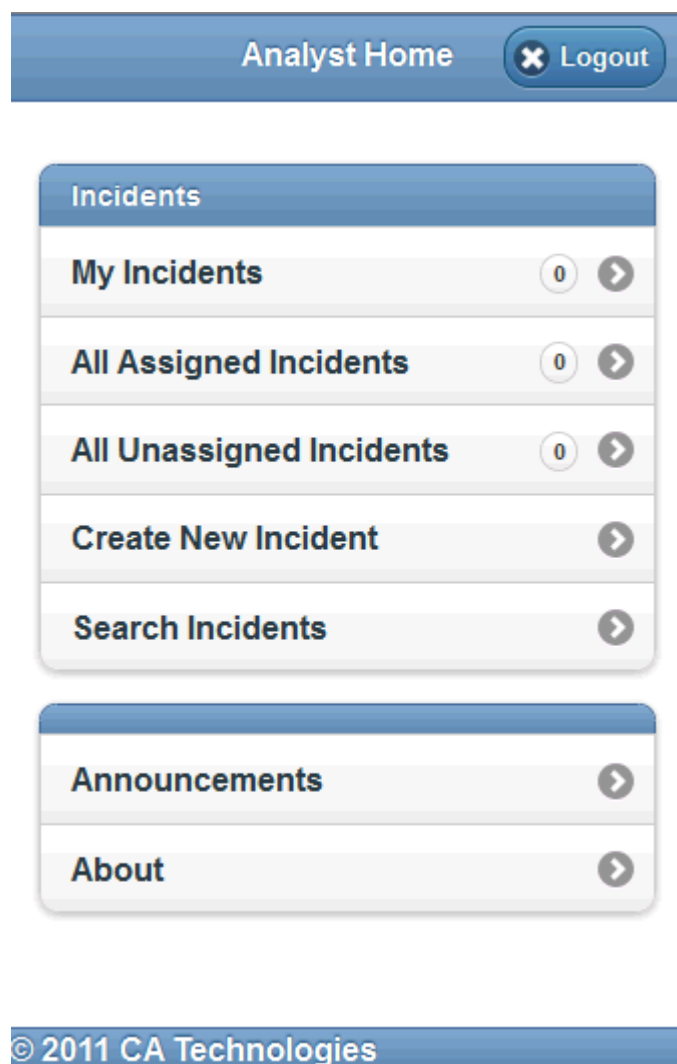
   Viene visualizzata la pagina di accesso all'interfaccia mobile REST di esempio.

2. Accedere a CA SDM con le proprie credenziali.

   Viene visualizzata la pagina principale dell'analista mobile REST.

3. Selezionare Incidenti assegnati.
4. Selezionare un incidente, ad esempio l'incidente 30.
5. Selezionare Crea attività nella pagina dei dettagli.
6. Selezionare Registra commento dall'elenco a discesa.
7. Selezionare Sì dall'opzione Interno.
8. Inserire un commento e selezionare Salva.

Esempio: Pagina iniziale dell'interfaccia Analista

L'immagine seguente mostra la pagina iniziale dell'interfaccia analista mobile REST di esempio:

Esempio: Pagina iniziale dell'interfaccia Dipendente

L'immagine seguente mostra la pagina iniziale dell'interfaccia dipendente mobile REST di esempio:

Esempio: Creazione di un Incidente da parte di un dipendente

In questo esempio, un dipendente esegue l'accesso all'interfaccia REST sul server per creare un Incidente per un problema di rete rilevato sul computer.

Procedere come descritto di seguito:

1. Il dipendente esegue l'accesso all'interfaccia mobile REST.
2. Il dipendente seleziona Crea nuovo Incidente.
3. Il dipendente completa le informazioni seguenti:
   - Immette il proprio numero di telefono
   - Immette il proprio indirizzo di posta elettronica
   - (Obbligatorio) Dall'elenco a discesa Urgenza, seleziona 3-Rapidamente
   - Immette **Rete** come area Incidente
   - Immette un riepilogo dell'Incidente

     Ad esempio, nel riepilogo è possibile segnalare che il dipendente non è in grado di accedere alla rete aziendale da un computer portatile.
   - (Obbligatorio) Immette una descrizione dell'Incidente

     Ad esempio, nella descrizione è possibile specificare il nome del computer portatile dell'utente finale nei dettagli hardware e di rete.
4. Il dipendente seleziona Salva.

   L'Incidente viene creato e viene visualizzato un messaggio contenente il numero di Incidente.

Capitolo 4: Configurazione di CA SDM Mobile Enabler

La distribuzione di CA SDM Mobile Enabler r2.0 viene eseguita con CA SDM Versione 12.9. L'utente amministratore deve eseguire alcune operazioni di configurazione per consentire agli utenti di utilizzare l'applicazione mobile.

Questa sezione contiene i seguenti argomenti:

CA SDM Mobile Enabler (a pagina 93)
Verifica dei prerequisiti (a pagina 99)
Applicazione delle patch per Open Space (a pagina 100)
(Facoltativo) Impostazione dei campi del modulo come non obbligatori (a pagina 102)
(Facoltativo) Applicazione della compatibilità delle approvazioni dopo l'aggiornamento (a pagina 103)
Accedere a CA SDM Mobile Enabler (a pagina 103)

CA SDM Mobile Enabler

CA SDM Mobile Enabler è un'interfaccia comune per accedere ad alcune delle funzioni principali di CA SDM e Open Space dal dispositivo mobile. Le seguenti funzionalità mobili sono disponibili in CA SDM Mobile Enabler:

- Coda analista (a pagina 94) - Consente di visualizzare ed eseguire attività nei ticket creati in CA SDM.
- Approvazioni (a pagina 95) - Consente di approvare o rispondere a elementi di lavoro assegnati creati da un modulo del flusso di lavoro.
- Open Space (a pagina 98) - Consente di pubblicare domande o fornire risposte nelle community. Se la community non è in grado di rispondere alle domande, è possibile generare un ticket.

È possibile scegliere le funzionalità che si desidera utilizzare dalla pagina di accesso quando si accede a CA SDM Mobile Enabler. Inoltre è possibile abilitare o disabilitare una funzionalità dopo aver effettuato l'accesso. Accedere alla schermata Impostazioni e toccare Add/Remove Capabilities (Aggiungi/Rimuovi funzionalità). Solo le funzionalità aggiunte in Mobile Enabler vengono visualizzate nella propria selezione. Passare il dito sulla schermata per attivare la funzionalità, immettere le credenziali, toccare Accesso.

Coda analista

La funzionalità Coda analista consente all'utente connesso di accedere alle seguenti funzionalità principali di CA SDM:

- Visualizzare il numero di ticket nella schermata principale di CA SDM quando si effettua l'accesso (solo Incidenti, Richieste, Problemi, Issue e Ordini di cambiamento). Il conteggio delle notifiche in ogni riquadro visualizza i conteggi dei ticket nuovi e aggiornati in seguito all'ultimo aggiornamento.

  Nota: la schermata principale non visualizza tutti i ticket da CA SDM. Per impostazione predefinita vengono visualizzati tutti i ticket assegnati a tutti gli utenti. È possibile modificare questo filtro predefinito.

- Toccare un riquadro del tipo di ticket dalla schermata principale per visualizzare l'elenco dei ticket. Filtrare ciascun tipo di ticket per visualizzare solo le informazioni selezionate. Ad esempio, toccare l'icona Filtro dall'elenco degli Incidenti e selezionare Assegnato - Priorità Alta. L'elenco viene aggiornato per visualizzare solo gli Incidenti selezionati.

  Nota: i filtri personalizzati sul server CA SDM e visualizzati nel contatore di CA SDM vengono visualizzati anche in questa funzionalità.

- Ricerca di ticket. Toccare l'area di ricerca e immettere la parola chiave per la ricerca. I risultati della ricerca vengono visualizzati durante la digitazione. È possibile cercare un ticket in base al numero o al riepilogo del ticket.

- Toccare un ticket per visualizzare i dettagli. È possibile visualizzare anche gli allegati e i registri attività (se presenti).

- Toccare Altre azioni (icona a forma di freccia nell'angolo in alto a destra della funzionalità) per eseguire azioni su un ticket:

  - Delegare o aggiornare lo stato o trasferire il ticket a un altro utente.
  - Aggiungere un commento al ticket.
  - Aggiungere un allegato al ticket. Le dimensioni consentite per l'allegato sono di massimo 3 MB.
    - Utilizzare la fotocamera per acquisire una snapshot.
    - Utilizzare la galleria per selezionare un'immagine (questa funzionalità supporta solo i formati immagine .jpeg, .jpg .png).

    Importante. Per visualizzare gli allegati dall'applicazione Web di CA SDM Mobile Enabler, disattivare l'opzione "Blocca popup" del browser Web.

- Modificare l'intervallo di aggiornamento (per impostazione predefinita è impostato su 4 minuti). Toccare il menu di sistema, Impostazioni, Capability Specific Settings (Impostazioni specifiche della funzionalità). Aumentare (segno più (+)) o diminuire (segno meno (-)) l'intervallo di polling.
- Scegliere le funzioni da visualizzare in questa funzionalità. Ad esempio, l'utente connesso può scegliere di visualizzare solo gli Incidenti. Accedere alla schermata Impostazioni e toccare Add/Remove Features (Aggiungi/Rimuovi funzioni). Passare il dito sulla schermata per attivare o disattivare una funzione.

Approvazioni

La funzionalità Approvazioni viene utilizzata per rispondere velocemente e con facilità alle attività del flusso di lavoro in sospeso. La funzionalità Approvazioni fornisce all'utente mobile tutte le informazioni necessarie per completare l'attività.

L'utente connesso può accedere alle seguenti funzioni principali della funzionalità:

- Visualizzare l'introduzione alla funzionalità. È possibile scegliere di *non* visualizzare questa introduzione quando si utilizza la funzionalità per la prima volta. Se si desidera visualizzare di nuovo l'introduzione, accedere a Impostazioni, Capability Specific Settings (Impostazioni specifiche della funzionalità) per la sezione Approvazioni e selezionare la casella di controllo Show Product Tour (Visualizza introduzione al prodotto).
- Visualizzare le seguenti attività:
  - Attività in sospeso dai seguenti moduli del flusso di lavoro che sono integrati con CA SDM:
    - Flusso di lavoro classico di CA SDM
    - IT Process Automation Manager (ITPAM)
    - CA Workflow (CAWF)

- Attività del flusso di lavoro che sono assegnate all'utente. Se l'utente connesso appartiene al gruppo PAMAdmins, può visualizzare e rispondere a qualsiasi attività ITPAM dalla funzionalità Approvazioni.
- Attività del flusso di lavoro che sono assegnate a un gruppo a cui l'utente appartiene.
  - Per il flusso di lavoro classico di CA SDM, le attività assegnate al gruppo di CA SDM non vengono visualizzate, solo le attività assegnate agli individui vengono visualizzate.
  - Se l'utente connesso appartiene al gruppo PAMAdmins, può visualizzare e rispondere a qualsiasi attività ITPAM dalla funzionalità Approvazioni.
- Attività del flusso di lavoro per cui all'utente viene chiesto di rispondere, a prescindere dall'assegnatario o dal richiedente del ticket di CA SDM. Ad esempio, è probabile che un'attività di approvazione finanziaria venga eseguita dall'utente che non è direttamente coinvolto con CA SDM.

Nota: se un modulo del flusso di lavoro non è attivo e l'utente non sta utilizzando il rispettivo elemento di lavoro, la funzionalità Approvazioni non visualizza gli elementi di lavoro né un messaggio di errore. Se in qualsiasi momento, il modulo del flusso di lavoro comincia a funzionare, l'utente visualizza i relativi elementi di lavoro. Ma se si sta già utilizzando un elemento di lavoro e il server si spegne, la funzionalità Approvazioni visualizza un report di errore.

- Visualizzare un grafico a barre che visualizza il numero di attività in sospeso che stanno aspettando l'input, in base il tempo di attesa. Questo grafico a barre consente all'utente di identificare nuove attività, oltre a determinare visivamente da quanto tempo sono in attesa.
- Visualizzare l'elenco delle attività filtrate in base al tempo di attesa. Toccare la barra sul grafico o utilizzare l'elenco a discesa nella parte superiore della schermata. Ad esempio, toccando Last Hour (Ultima ora) la barra visualizza tutte le attività create o modificate nell'ultima ora e in attesa di approvazione.
- Ricerca di un'attività in sospeso; immettere il testo di ricerca nell'area Ricerca. Il risultato della ricerca viene aggiornato durante la digitazione. È possibile effettuare la ricerca mediante i numeri dei ticket, la priorità o parole chiave contenute nelle descrizioni delle attività.
- Visualizzare i dettagli dell'elemento di lavoro toccando un'attività nell'elenco. Quando si visualizzano i dettagli, è possibile eseguire le azioni seguenti:
  - Visualizzare il modulo di input dell'elemento di lavoro, quasi uguale a quello del modulo del flusso di lavoro. I moduli di approvazione personalizzati sono automaticamente disponibili sul dispositivo mobile senza alcuna modifica. Vengono riformattati per il rendering sul dispositivo mobile.
  - Capire di più dell'elemento di lavoro toccando l'icona del ticket per visualizzare le informazioni relative al ticket di CA SDM. Queste informazioni possono includere motivazioni di business, procedure di implementazione e backout, contatto, assegnatario, informazioni, priorità, SLA, gravità, ecc.

- Chiamare o inviare un messaggio di posta elettronica al richiedente, assegnatario eccetera toccando il numero di telefono o l'indirizzo di posta elettronica elencato nella rispettiva scheda del ticket. Queste informazioni vengono visualizzate solo se il ticket di CA SDM contiene queste informazioni di contatto.
- Scaricare e visualizzare gli allegati per il rispettivo ticket di Ordine di cambiamento. Potrebbe essere necessario installare sul dispositivo mobile un software di visualizzazione aggiuntivo per aprire il documento scaricato.

  Importante. Per visualizzare gli allegati dall'applicazione Web di CA SDM Mobile Enabler, disattivare l'opzione "Blocca popup" del browser Web.

  Nota: se si scarica l'allegato sul browser a comparsa di Android, viene visualizzato un messaggio di errore. Toccare la freccia sul lato sinistro del browser a comparsa. Il browser a comparsa viene convertito nel browser principale ed è possibile scaricare l'allegato.
- Rispondere all'elemento di lavoro immettendo le informazioni richieste nel modulo dettagli e toccare Invia. L'attività successiva viene aperta automaticamente per ricevere una risposta, nel caso in cui siano presenti più attività in sospeso. È possibile toccare anche la freccia in avanti nell'angolo in alto a destra della funzionalità per aprire l'elemento di lavoro successivo.

■ Su richiesta del supporto, abilitare le informazioni di debug selezionando il menu di sistema, Impostazioni, Capability Specific Settings (Impostazioni specifiche della funzionalità). Toccare l'elenco a discesa Tracing (Traccia) per selezionare un'opzione. Scegliere l'opzione "attivo" per abilitare le informazioni di debug. Scegliere l'opzione "dettagliato" per ottenere informazioni più dettagliate. È possibile visualizzare le informazioni di accesso nella directory $NX_ROOT\log\approve.log sul server CA SDM. Si consiglia di disattivare l'opzione per evitare il sovraccarico di un server aggiuntivo una volta completata la sessione di supporto.

■ Cambiare il formato data/ora toccando il menu di sistema, Impostazioni, Capability Specific Settings (Impostazioni specifiche della funzionalità) e scegliendo un Date Time Format (Formato data/ora). Il formato data/ora cambiato si riflette solo dopo aver aggiornato la funzionalità.

■ Aggiornare l'elenco attuale degli elementi di lavoro toccando il menu di sistema nell'angolo in alto a destra della pagina dell'elenco attività e scegliere Aggiorna.

■ Cambiare l'intervallo di tempo di aggiornamento che specifica la frequenza con cui il riquadro Approvazioni viene aggiornato, cambiando l'intervallo di polling individuato nella pagina Capability Specific Settings (Impostazioni specifiche della funzionalità).

- Abilitare l'opzione di timeout della risposta per cui l'utente connesso riceve un messaggio se la funzionalità non risponde entro un periodo di tempo specificato. Come utente connesso, è possibile impostare questa intervallo (in minuti) dal menu di sistema, Impostazioni, Capability Specific Settings (Impostazioni specifiche della funzionalità). L'opzione Timeout in minuti è impostata su due minuti per impostazione predefinita. È possibile aumentare (segno più (+)) o diminuire (segno meno (-)) questo intervallo. Se la funzionalità non risponde entro il timeout pianificato, l'utente connesso visualizza un messaggio di errore. Dopo avere fatto clic su OK nel prompt del messaggio, l'utente viene reindirizzato alla pagina di accesso della funzionalità Approvazioni.

Open Space

La funzionalità Open Space consente all'utente connesso di accedere alle seguenti funzioni principali di CA Open Space su un dispositivo mobile:

- Visualizzare il conteggio delle ultime domande sulla schermata principale, che vengono pubblicati da CA Open Space. Le pubblicazioni vengono classificate in base a tag come Consigliato, Latest (Più recente), Following, ecc. Per impostazione predefinita vengono visualizzate le domande più recenti.
- (Se CA Open Space è configurato con CA SDM) Visualizzare il conteggio dei ticket (Richiesta o Incidente, in base alla configurazione effettuata dall'amministratore di sistema sul server CA Open Space) nella schermata principale, che l'utente ha cerato mediante tale funzionalità.
- Toccare il riquadro della domanda dalla schermata principale per visualizzare le pubblicazioni correlate. Selezionare un'opzione, ad esempio Latest (Più recente), dall'elenco a discesa per visualizzare solo le ultime pubblicazioni.
- Cercare una pubblicazione da tutte le origini. Immettere i criteri di ricerca nella casella di testo Cerca e toccare Invio. I risultati della ricerca vengono visualizzati da tutte le origini. Dall'elenco a discesa è possibile selezionare Globale per eseguire la ricerca in tutte le origini dati abilitate sul server CA Open Space o selezionare Domande per eseguire la ricerca nelle domande elencate nella funzionalità.
- Cercare richieste o Incidenti.
- Toccare una domanda per visualizzare la pubblicazione dettagliata. Toccare Altre azioni (icona a forma di freccia nell'angolo in altro a destra della funzionalità) per eseguire le azioni seguenti:
  - Rispondere alla pubblicazione
  - Seguire o smettere di seguire la pubblicazione
  - Condividere la pubblicazione
  - Aprire un ticket Service Desk se la pubblicazione non fornisce una risposta alle proprie domande.

Nota: per aggiungere nuovi campi nel modulo della richiesta, l'amministratore di sistema deve configurare i campi sul server CA Open Space. Gli stessi campi configurati vengono visualizzati nella funzionalità Open Space. Il numero di campi configurabili sul server CA Open Space è 5. Per ulteriori informazioni su come configurare i campi, consultare la *Guida per l'amministratore di CA Open Space*.

- Cambiare l'intervallo di aggiornamento (per impostazione predefinita è impostato su quattro minuti). Toccare il menu di sistema, Impostazioni, Capability Specific Settings (Impostazioni specifiche della funzionalità). Aumentare (segno più (+)) o diminuire (segno meno (-)) l'intervallo di polling.
- Scegliere le funzioni da visualizzare in questa funzionalità. Ad esempio, l'utente connesso può scegliere di visualizzare solo le domande. Accedere alla schermata Impostazioni e toccare Add/Remove Features (Aggiungi/Rimuovi funzioni). Passare il dito sulla schermata per attivare o disattivare una funzione.

Verifica dei prerequisiti

Verificare i requisiti seguenti prima di configurare CA SDM Mobile Enabler:

- Sistemi operativi mobili certificati (a pagina 99)
- Per accedere alle funzionalità Coda analista e Approvazioni, è necessario installare e configurare CA SDM Versione 12.9 sul server in cui si desidera installare CA SDM Mobile Enabler. Anche REST viene installato e configurato sullo stesso server. Per ulteriori informazioni, consultare la *Guida all'implementazione di CA Service Desk Manager*.
- Per accedere a funzionalità Open Space, è necessario installare CA Open Space r2.0 e configurarlo nel server CA SDM. Per ulteriori informazioni, consultare la *Guida all'implementazione di CA Open Space*.
- Associare gli utenti connessi alla funzionalità Coda analista con il ruolo API del servizio Web REST. Accertarsi che gli accessi alle funzioni *Amministrazione*, *Protezione* e *Riferimento* di questo ruolo vengano assegnati con i ruoli di accesso Visualizzazione o Modifica. Per ulteriori informazioni sull'accesso alle funzioni, sul livello di accesso e sui ruoli, consultare la *Guida per l'amministratore* di *CA Service Desk Manager*.

Sistemi operativi mobili certificati

CA SDM Mobile Enabler è certificato sul browser nativo per i sistemi operativi mobili seguenti:

- iOS 5.1 e versioni successive
- Android 4.x

Applicazione delle patch per Open Space

In funzione del sistema operativo installato, applicare le patch seguenti sul server CA Open Space prima di effettuare la distribuzione di CA SDM Mobile Enabler per accedere alla funzionalità Open Space:

Sistema operativo	Numero della patch
Windows	RO61737
Linux	RO61738

Abilitazione delle impostazioni CORS

Abilitare le impostazioni CORS (cross - origin resource sharing) per utilizzare la funzionalità mobile Open Space.

Importante. Questo processo è adatto solo all'applicazione basata su Web e *non* all'applicazione nativa di CA SDM Mobile Enabler.

Procedere come descritto di seguito:

1. Prima di abilitare le impostazioni CORS, verificare che le patch relative a Open Space (a pagina 100) siano state applicate.
2. Accedere al server Open Space.
3. Accedere alla seguente directory:

   `OSOP_HOME/tomcat.7.xx/webapps/ROOT/WEB-INF`
4. Aprire il file web.xml.
5. Aggiungere il contenuto seguente dopo l'ultimo tag </filter> nel file XML:

```
<filter>
<filter-name>CORS</filter-name>
<filter-class>com.thetransactioncompany.cors.CORSFilter</filter-class>
<init-param>
<param-name>cors.allowGenericHttpRequests</param-name>
<param-value>true</param-value>
</init-param>
```

```
<init-param>
<param-name>cors.allowOrigin</param-name>
<param-value>*</param-value>
</init-param>
<init-param>
<param-name>cors.allowSubdomains</param-name>
<param-value>true</param-value>
</init-param>
<init-param>
<param-name>cors.supportedMethods</param-name>
<param-value>GET, HEAD, POST, OPTIONS, PUT, DELETE</param-value>
</init-param>

<init-param>
<param-name>cors.supportedHeaders</param-name>
<param-value>Origin, Accept, Authorization, Content-Type,
X-Requested-With</param-value>
</init-param>
<init-param>
<param-name>cors.exposedHeaders</param-name>
<param-value>X-Test-1, X-Test-2</param-value>
</init-param>
<init-param>
<param-name>cors.supportsCredentials</param-name>
<param-value>true</param-value>
</init-param>

<init-param>
<param-name>cors.maxAge</param-name>
<param-value>3600</param-value>
</init-param>
</filter>
<filter-mapping>
<filter-name>CORS</filter-name>
<url-pattern>*</url-pattern>
</filter-mapping>
```

6. (Facoltativo) Se si desidera un dominio specifico per accedere al server <osop>, completare i passaggi seguenti:

   a. Accedere alla linea seguente nel file XML:

      ```
      <init-param>

      <param-name>cors.allowOrigin</param-name>

      <param-value>*</param-value>

      </init-param>
      ```

b. Sostituire cors.allowOrgin param-value con le seguenti informazioni di sottodominio del server CA SDM:

```
http://<server_Name>:<Port_Number>
```

Nota: è possibile aggiungere più sottodomini, separati da uno spazio.

7. Salvare il file.
8. Riavviare il server Open Space.

   Le impostazioni CORS sono abilitate.

(Facoltativo) Impostazione dei campi del modulo come non obbligatori

Per impostazione predefinita, tutti i campi di input nella funzionalità Approvazioni che vengono derivati dal modulo del flusso di lavoro ITPAM sono obbligatori. A seconda della versione ITPAM installata, l'amministratore di sistema può rendere questi campi non obbligatori.

Procedere come descritto di seguito:

1. Accedere al server CA SDM e aprire il file NX.env.
2. Aggiungere la variabile seguente in questo file:

   ```
   NX_MOBILE_WFM_ITPAM_ALL_FIELDS_ARE_REQUIRED
   ```

3. Impostare il valore variabile.
4. Salvare il file.
5. A seconda del valore variabile e della versione ITPAM, i cambiamenti seguenti sono applicabili:
   - Se la variabile non è impostata, tutti i campi da ITPAM 3.1, 4.0 o versioni successive diventano obbligatori per impostazione predefinita.
   - Se il valore variabile viene impostato su Sì, tutti i campi da ITPAM 3.1, 4.0 o versioni successive diventano obbligatori.
   - Se il valore variabile viene impostato su No, tutti i campi da ITPAM 3.1 seguono il vincolo di lunghezza minima e massima. La lunghezza minima e massima per campi di input stringa in ITPAM 4.0 o versioni successive non sono applicabili alla funzionalità Approvazioni. Pertanto tutti i campi diventano non obbligatori, se il valore variabile viene impostato su No.

(Facoltativo) Applicazione della compatibilità delle approvazioni dopo l'aggiornamento

Affinché gli utenti accedano alla funzionalità Approvazioni più recente con le ultime funzioni e possano beneficiare di un'esperienza coerente, impostare la variabile NX_MOBILE_WFM_FORCE_CLIENTVERSION_UPGRADE su **Sì**.

Quando l'opzione è impostata, agli utenti che tentano di accedere alla versione precedente della funzionalità Approvazioni viene richiesto di aggiornare la funzionalità e l'accesso viene negato.

Procedere come descritto di seguito:

1. Accedere al server CA SDM e aprire il file NX.env.
2. Aggiungere la variabile seguente in questo file:

   `NX_MOBILE_WFM_FORCE_CLIENTVERSION_UPGRADE`
3. Impostare il valore variabile su Sì.
4. Salvare il file.
5. Riavviare il server CA SDM.

Accedere a CA SDM Mobile Enabler

Per accedere all'applicazione usdk> Mobile Enabler da un *dispositivo mobile*, utilizzare l'URL seguente:

```
http(s)://<CA_SDM_Server_Name>:<REST_Port_Number>/casdm
```

Nota: comunicare agli utenti questo URL se desiderano utilizzare l'applicazione Web di CA SDM Mobile Enabler sul dispositivo mobile.

Se si desidera utilizzare CA SDM Mobile Enabler come *applicazione mobile nativa* sul dispositivo mobile, effettuare le operazioni seguenti:

1. Accedere a Google Play (per gli utenti di Android) o App Store (per utenti di iOS).
2. Cercare CA Service Desk Manager.
3. Installare l'applicazione CA Service Desk Manager.

   L'icona di CA SDM viene visualizzata nel telefono cellulare una volta completata correttamente l'installazione.

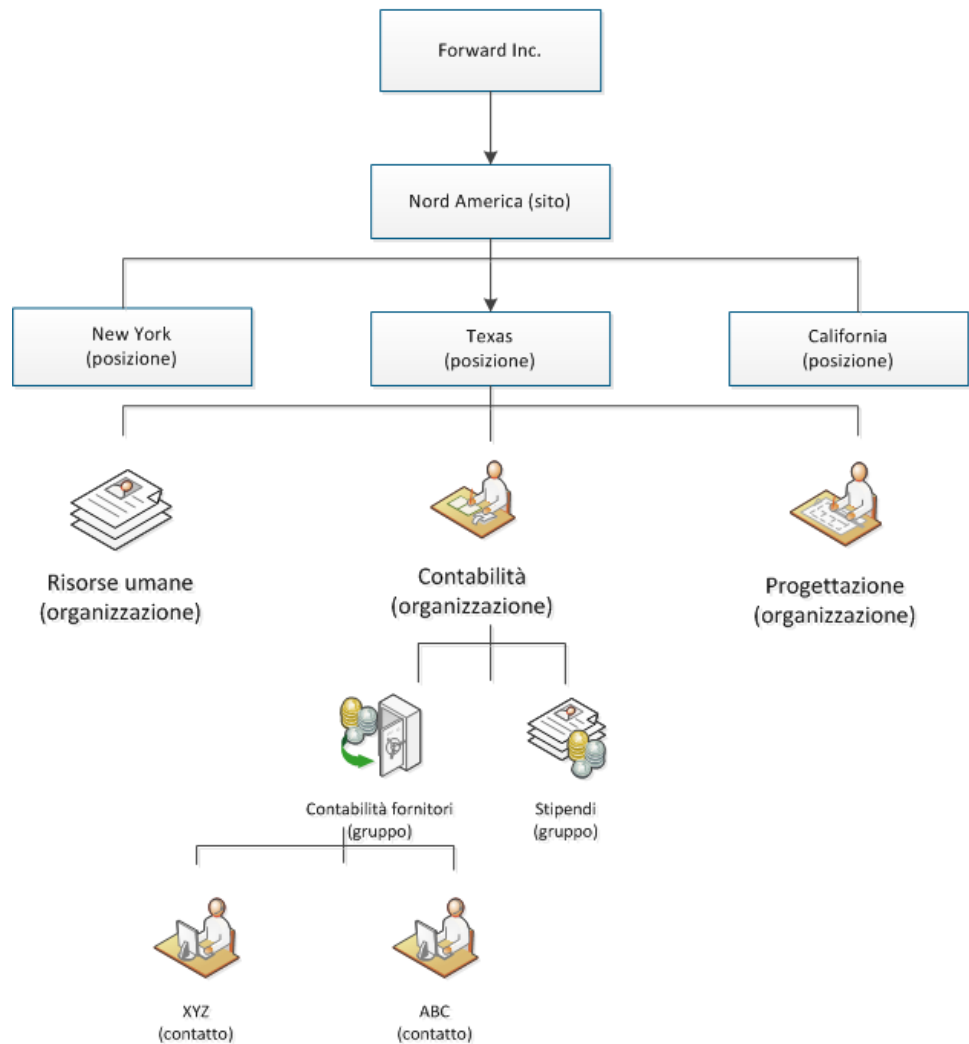
Creazione della struttura aziendale

Una struttura aziendale è una rappresentazione personalizzata e logica della propria organizzazione in un ambiente di Unicenter Service Desk. Questo scenario descrive come un amministratore può creare la struttura aziendale di un'organizzazione per gestire e tenere traccia di contatti, gruppi e asset distribuiti in varie posizioni. Una volta creata una struttura aziendale, è possibile generare report per analizzare richieste in base al sito, l'organizzazione o il gruppo.

Esempio

L'azienda inventata Forward, Inc. utilizza un sistema di elaborazione delle richieste per più uffici distribuiti in varie posizioni geografiche. L'azienda progetta di implementare Unicenter Service Desk per analizzare il numero e il tipo di richieste che vengono generate dai suoi vari segmenti di business.

Il diagramma seguente illustra l'esempio di una struttura aziendale di alto livello utilizzando l'azienda inventata Forward, Inc.

Esempio di struttura aziendale
Forward Inc.
Nord America (sito)
New York
(posizione)
Texas
(posizione)
California
(posizione)
Risorse umane
(organizzazione)
Contabilità
(organizzazione)
Progettazione
(organizzazione)
Contabilità fornitori
(gruppo)
Stipendi
(gruppo)
XYZ
(contatto)
ABC
(contatto)

Per facilitare un monitoraggio e un processo decisionale efficaci, l'organizzazione deve tenere traccia degli elementi seguenti:

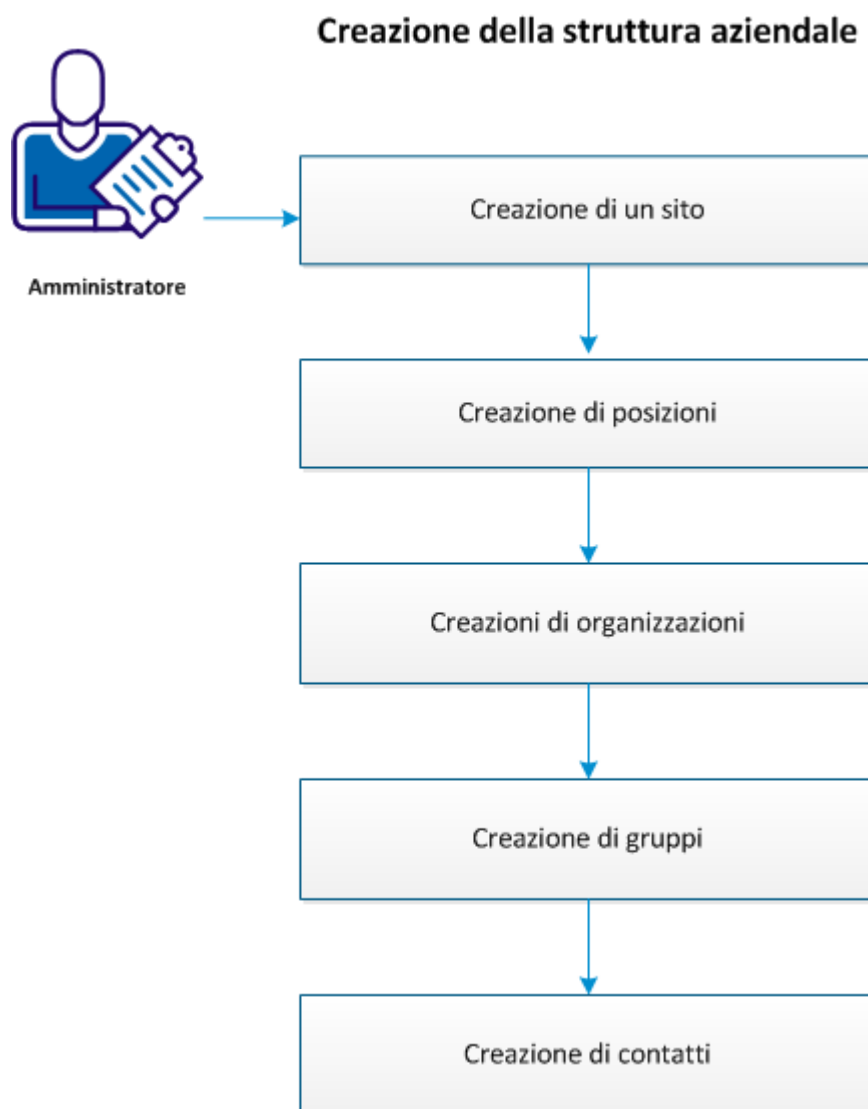
- Contatti, gruppi di contatto e posizioni
- Asset nelle varie posizioni

La creazione di una struttura aziendale permette al team di gestione in Forward, Inc. di eseguire le azioni seguenti:

- Generare rapporti per analizzare le richieste in base al sito, l'organizzazione e il gruppo
- Aumentare l'efficienza complessiva implementando misure correttive per ciascun difetto presente nel processo di richiesta

Modalità di creazione della struttura aziendale

Per creare una struttura aziendale, si definisce una gerarchia logica dei siti e delle organizzazioni all'interno dell'azienda, quindi si associano contatti e gruppi ai rispettivi siti e organizzazioni.

Il diagramma seguente mostra come un amministratore può definire gli oggetti in una struttura aziendale tipica:

Procedere come descritto di seguito:

1. Creazione di un sito (a pagina 110)
2. Creazione di posizioni (a pagina 111)
3. Creazione di organizzazioni (a pagina 112)
4. Creazione di gruppi (a pagina 113)
5. Creazione di contatti (a pagina 114)

Creazione di un sito

Un sito è una regione geografica in cui la propria organizzazione ha una o più posizioni.

Ad esempio, il Nord America può essere un sito, con posizioni (uffici) a New York, in California e in Texas.

Nota: In caso di abilitazione dell'opzione multi-tenancy, selezionare il titolare appropriato dall'elenco a discesa.

Procedere come descritto di seguito:

1. Selezionare File, Nuovo sito dalla barra dei menu nel Contatore di Unicenter Service Desk.

   Viene visualizzata la finestra Crea Nuovo sito.

2. Immettere le informazioni specifiche per il proprio sito.
3. Fare clic su Salva.

   Il record del sito viene creato e salvato.

Creazione di posizioni

Una posizione è un posto fisico, come ad esempio l'indirizzo di un ufficio. Ad esempio, gli indirizzi degli uffici di New York, della California e del Texas possono essere posizioni sotto il sito Nord America.

La creazione di posizioni consente di gestire contatti e risorse in quella posizione. Una volta creata una posizione, è possibile assegnarla a un sito.

Procedere come descritto di seguito:

1. Selezionare File, Nuova posizione dalla barra dei menu nel Contatore.

   Viene visualizzata la pagina Crea Nuova posizione.

2. Immettere le informazioni specifiche per la propria posizione, quindi configurare la posizione mediante i controlli seguenti sulle schede:

   Indirizzo

   Specifica l'indirizzo fisico della posizione.

   Assegnazione automatica

   Assegna automaticamente i ticket (richieste, ordini di cambiamento e questioni) ai membri in questa posizione.

   Aggiorna aree richiesta

   Selezionare le aree di richiesta che si desidera assegnare ai membri della posizione automaticamente.

   Aggiorna categorie modifica

   Selezionare le categorie di modifica che si desidera assegnare a membri della posizione.

   Aggiorna categorie questione

   Selezionare le categorie di questione che si desidera assegnare a membri della posizione.

   Aggiorna gruppi

   Selezionare i gruppi che si desidera aggiornare per l'assegnazione automatica dei ticket.

   Importante: Dopo avere aggiornato le aree di richiesta e delle categorie, abilitare l'assegnazione automatica individualmente per ciascuna area di richiesta e categoria.

3. Fare clic su Salva.

   I dettagli della posizione vengono salvati.

4. (Facoltativo) Ripetere i passaggi da 1 a 3 per aggiungere più posizioni.

Creazione di organizzazioni

Un'organizzazione fa riferimento a un dipartimento o divisione interni o a un'azienda esterna. È possibile assegnare le organizzazioni a ticket, classi di elementi della configurazione e contatti.

Ad esempio, è possibile definire elementi della configurazione per le organizzazioni, che specificano i componenti hardware, software e i servizi da esse utilizzati.

Nota: In caso di abilitazione dell'opzione multi-tenancy, selezionare il titolare appropriato dall'elenco a discesa.

Procedere come descritto di seguito:

1. Selezionare File, Nuova organizzazione dalla barra dei menu nel Contatore.

   Viene visualizzata la pagina Crea Nuova organizzazione.

2. Immettere le informazioni specifiche per la propria organizzazione, quindi specificare i dettagli dell'organizzazione nei campi seguenti:

   Indirizzo

   Viene visualizzato l'indirizzo della posizione a cui si associa l'organizzazione. I campi vengono popolati automaticamente quando si assegna la posizione all'organizzazione.

   Ambiente

   Vengono visualizzati gli elementi della configurazione (ad esempio, attrezzatura, software e servizi) utilizzati dall'organizzazione. È possibile associare uno o più elementi della configurazione all'organizzazione. Associare gli elementi della configurazione all'organizzazione aiuta gli amministratori a tenere traccia delle risorse utilizzate dalle organizzazioni nelle varie posizioni.

3. Fare clic su Salva.

   I dettagli dell'organizzazione vengono salvati.

4. (Facoltativo) Ripetere i passaggi da 1 a 3 per aggiungere più organizzazioni.

Creazione di gruppi

Un gruppo è una raccolta di contatti che rappresenta un'area specifica di responsabilità. La definizione dei gruppi consente di assegnare la responsabilità della risoluzione di un ticket quando tale responsabilità è condivisa tra più persone. Ad esempio, il gruppo Risorse umane di Dallas è responsabile della gestione delle Issue relative al personale dell'ufficio di Dallas dell'organizzazione. Quando un dipendente di questo ufficio ha un problema, è possibile assegnarlo al gruppo Risorse umane di Dallas per la risoluzione.

Nota: In caso di abilitazione dell'opzione multi-tenancy, selezionare il titolare appropriato dall'elenco a discesa. L'opzione pubblica (condivisa) consente di creare l'oggetto per tutti i titolari.

Procedere come descritto di seguito:

1. Selezionare File, Nuovo gruppo dalla barra dei menu nel Contatore.

   Viene visualizzata la pagina Crea Nuovo gruppo.

2. Immettere le informazioni specifiche per questo gruppo e per la propria organizzazione indicando i dettagli del gruppo nei campi seguenti:

   Notifica

   Definisce le informazioni di contatto e il metodo di notifica del gruppo.

   Indirizzo

   Assegna il gruppo a una posizione.

   Informazioni organizzazione

   Specifica l'organizzazione funzionale o amministrativa, il reparto, il centro di costo o le informazioni sul vendor.

   Ambiente

   Specifica l'ambiente (ad esempio, attrezzature, software e servizi).

   Membri

   Aggiunge o rimuove contatti.

   Contratti del servizio

   Elenca contratti del servizio associati al gruppo.

   Assegnazione automatica

   Elenca le assegnazioni automatiche dei ticket in base all'appartenenza ai gruppi.

   Commenti e gestione speciale

   Elenca i commenti e i tipi di gestione speciale, ad esempio i tipi VIP o i tipi di rischio di protezione. È possibile fare clic su Aggiorna Gestioni speciali del contatto per cercare membri di gestione specifici.

3. Fare clic su Salva.

Il record del gruppo viene salvato e viene visualizzata la pagina Dettagli gruppo. i pulsanti seguenti diventano disponibili per configurare il gruppo.

Aggiorna ambiente

Nella scheda Dettagli di contatto, Ambiente fare clic sul pulsante per visualizzare la finestra Ricerca Elemento della configurazione per il gruppo. È possibile specificare i criteri di ricerca per gli asset che si desidera includere in questa pagina. È possibile creare un nuovo elemento della configurazione e gli asset di ricerca mediante la finestra Aggiorna o Contatti, rispettivamente.

Aggiorna membri

Nella scheda Membri, Contratti del servizio, Assegnazione automatica, Membri, questo pulsante consente di visualizzare i contatti. È possibile aggiungere e rimuovere contatti di questo gruppo.

4. (Facoltativo) Ripetere i passaggi da 1 a 3 e aggiungere più gruppi a seconda delle esigenze.

Creazione di contatti

Un contatto è una persona che utilizza il sistema regolarmente, ad esempio un analista o un cliente. Una volta creati la struttura aziendale e i gruppi, creare i contatti ed eseguirne il mapping alla rispettiva posizione e organizzazione.

È possibile creare contatti nei modi seguenti:

- Creazione di contatti manuale

  Utilizzare questo metodo se si desidera creare contatti mediante il Contatore di CA SDM.

- Utilizzo di dati dal database LDAP

  Utilizzare questo metodo se l'installazione di CA SDM è configurata per l'accesso a un server LDAP (Lightweight Directory Access Protocol) e CA SDM ha le opzioni necessarie installate.

Creazione di contatti manuale

Se non si desidera utilizzare una directory attiva come LDAP per le informazioni relative ai contatti, è possibile creare i contatti manualmente in CA SDM.

Nota: In caso di abilitazione dell'opzione multi-tenancy, selezionare il titolare appropriato dall'elenco a discesa.

Procedere come descritto di seguito:

1. Selezionare File, Nuovo contatto dalla barra dei menu nel Contatore.

   Viene visualizzata la finestra Crea Nuovo contatto.

2. Compilare i campi seguenti in modo appropriato per il contatto:

   Titolare

   Specifica il titolare che viene associato al contatto (per installazioni con più titolari).

   Contatta ID

   Specifica un identificatore univoco per il contatto. Se si utilizza l'autenticazione dell'utente predefinito, il valore in questo campo viene utilizzato come password quando l'utente effettua l'accesso.

   ID utente

   Specifica il nome utente del contatto. Il contatto utilizza questo valore per accedere al sistema.

   Tipo di servizio

   Specifica il livello del servizio di assistenza ricevuto dal contatto.

   Partizione dati

   Specifica la partizione dati del contatto. Questo valore determina i record a cui può accedere il contatto.

   Tipo di accesso

   Specifica il tipo di accesso. Il tipo di accesso determina le funzioni di sistema a cui può accedere il contatto.

   Disponibile

   Indica se il contatto è disponibile per assegnazioni di ticket.

   Conferma salvataggio self-service

   Indica se il contatto riceve una conferma quando si salva un record dall'interfaccia self-service.

   Gruppo titolare dell'analista

   (Solo Tipo contatto Analista) Specifica il gruppo di titolari di cui è responsabile l'analista.

3. Per configurare il contatto, utilizzare i controlli seguenti disponibili nelle schede.

Notifica

Definisce le informazioni di contatto e il metodo di notifica del contatto.

- Selezionare il metodo di notifica da utilizzare per il livello di urgenza di ogni messaggio per il contatto.

  Ad esempio, è possibile inviare al contatto le notifiche mediante il metodo Posta elettronica per le attività di livello normale e utilizzare il metodo Posta elettronica cercapersone per le attività con livello di emergenza.

- Selezionare il turno valido per ciascun livello di notifica di urgenza.

  Ad esempio, si può assegnare un turno Normale (cinque giorni a settimana per otto ore al giorno) alle notifiche di livello normale e un turno di 24 ore alle notifiche con livello di emergenza.

Indirizzo

Specifica l'indirizzo del contatto.

Informazioni organizzazione

Specifica l'organizzazione funzionale o amministrativa, il reparto, il centro di costo o le informazioni sul vendor del contatto.

Ambiente

Specifica l'ambiente del contatto, ad esempio apparecchiature, software e servizi.

Gruppi

Consente di assegnare un contatto a un gruppo, ovvero a una raccolta di contatti con un'area comune di responsabilità.

Ruoli

Consente di assegnare il contatto a uno o più ruoli.

Contratti del servizio

Visualizza eventuali contratti del servizio associati al contatto.

Gestione speciale

Elenca i contatti di gestione speciale e consente di cercare e associare un contatto, ad esempio un visitatore o un contatto con un tipo di rischio di protezione, a un tipo di gestione speciale.

Registro eventi

Elenca gli eventi associati al contatto, ad esempio attività di self-service o della conoscenza.

Attività

Visualizza il registro delle attività per il contatto.

4. Fare clic su Salva.

   Le informazioni sul contatto vengono salvate.

Utilizzo di contatti dal database LDAP

Se l'installazione del prodotto è configurata per l'accesso a un server LDAP (Lightweight Directory Access Protocol) e sono installate le opzioni necessarie, è possibile creare e aggiornare i contatti utilizzando i dati del database LDAP. Questa funzionalità facilita la sincronizzazione dei contatti con i dati utente di rete.

Attenersi alla procedura seguente:

1. Selezionare File, Nuovo contatto da LDAP dalla barra dei menu nel Contatore.

   Viene visualizzata la pagina Ricerca directory LDAP.

2. Immettere uno o più filtri per limitare l'elenco delle voci LDAP ai record specifici di interesse.

3. Fare clic su Cerca.

   La pagina Elenco voci LDAP mostra i record corrispondenti ai criteri di ricerca specificati.

4. Fare clic sulla voce LDAP per creare un contatto.

   Viene visualizzata la pagina Crea Nuovo contatto, parzialmente compilata con le informazioni LDAP.

5. Immettere eventuali informazioni aggiuntive.

6. Per configurare il contatto, utilizzare i controlli seguenti disponibili nelle schede.

   Notifica

   Definisce le informazioni di contatto e il metodo di notifica del contatto.

   Indirizzo

   Specifica l'indirizzo della posizione a cui si associa l'organizzazione.

   Informazioni organizzazione

   Specifica l'organizzazione funzionale o amministrativa, il reparto, il centro di costo o le informazioni sul vendor del contatto.

   Ambiente

   Specifica l'ambiente del contatto, ad esempio apparecchiature, software e servizi.

   Gruppi

   Consente di assegnare un contatto a un gruppo, ovvero a una raccolta di contatti con un'area comune di responsabilità.

   Ruoli

   Consente di assegnare il contatto a uno o più ruoli.

   Contratti del servizio

   Visualizza eventuali contratti del servizio associati al contatto.

Gestione speciale

Elenca i contatti di gestione speciale. È inoltre possibile cercare contatti o associare un contatto a un tipo di gestione speciale, ad esempio un visitatore o un tipo di rischio di protezione.

Registro eventi

Elenca gli eventi associati al contatto, ad esempio attività di self-service o della conoscenza.

Attività

Visualizza il registro delle attività per il contatto.

7. Fare clic su Salva.

   Le informazioni sul contatto vengono salvate.

8. (Facoltativo) Ripetere i passaggi da 1 a 7 per aggiungere più contatti.

È stata creata correttamente una struttura aziendale a cui sono associati contatti e gruppi. Ora è possibile generare report per analizzare le richieste in base al sito, l'organizzazione o il gruppo.

Definizione dell'infrastruttura aziendale

Un aspetto importante dell'implementazione del Service Desk tramite CA SDM è rappresentato dalla definizione dell'infrastruttura aziendale mediante la configurazione dei seguenti elementi:

- Famiglie e classi di elementi della configurazione
- Produttori e modelli
- Stati di servizio
- Vendor e tipi di vendor

Le seguenti informazioni forniscono una descrizione generale per ogni oggetto e illustrano la modalità di utilizzo dell'oggetto nel prodotto.

Nota: per ulteriori informazioni sulla definizione dei vari oggetti, vedere la *Guida in linea*.

Ordine di definizione degli oggetti

Quando si definiscono gli oggetti, occorre iniziare dai livelli inferiori della gerarchia di oggetti. In tal modo, quando si definiscono gli oggetti di livello superiore, è possibile selezionare oggetti esistenti nei livelli inferiori della gerarchia. Ad esempio, poiché una classe fa riferimento a una famiglia, è necessario definire in primo luogo le famiglie, quindi le classi. Allo stesso modo, poiché gli elementi della configurazione si trovano all'inizio della gerarchia, devono essere definiti per ultimi, dopo aver definito tutti gli oggetti di supporto. L'ordine di definizione degli oggetti dati è, pertanto, il seguente:

Definire come primo elemento	Definire come secondo elemento	Definire come terzo elemento
Famiglie	Classi	Elementi della configurazione
Produttori	Modelli	Elementi della configurazione
Stati di servizio	Elementi della configurazione	
Tipi di fornitore	Fornitori	Elementi della configurazione

Famiglie e classi

Le *famiglie* consentono di classificare gli elementi della configurazione per tipo e di assegnare a ciascuno attributi significativi. Le *classi* identificano le categorie generali di asset supportate dall'azienda. Le famiglie sono categorie generiche di elementi della configurazione come hardware, software e servizi. Le classi sono categorie più specifiche all'interno della famiglia. Ad esempio, la famiglia hardware può contenere classi quali modem, router, ripetitori e bridge.

L'organizzazione degli elementi della configurazione in famiglie e in classi ne facilita la gestione. Ad esempio, è possibile generare un elenco di elementi della configurazione appartenenti a una famiglia oppure a una classe specifica.

Produttori e modelli

I *produttori* identificano i produttori dei vari elementi della configurazione di interesse per l'azienda.I *modelli* contengono informazioni specifiche sui prodotti forniti all'azienda da un produttore. Ad esempio, è possibile definire come produttore una specifica società di software. Quindi, definire come modello ogni applicazione fornita all'azienda da tale società.

La definizione dei produttori e dei modelli facilita la gestione degli elementi della configurazione. Ad esempio, è possibile generare un elenco di modelli forniti da un produttore specifico e generare un elenco di elementi della configurazione di un particolare modello.

Stato servizio

Lo *stato di servizio* consente di identificare lo stato degli elementi della configurazione. Alcuni esempi di stati di servizio sono: *in servizio*, *in riparazione* o *sospeso*. La definizione degli stati di servizio consente di tenere traccia della disponibilità e dell'uso degli elementi della configurazione nell'azienda. Ad esempio, è possibile generare l'elenco degli elementi della configurazione attualmente in riparazione.

Tipi di fornitore e fornitori

I *tipi di fornitore* costituiscono la classificazione dei fornitori che identificano il tipo di società che fornisce gli elementi della configurazione. Ad esempio, è possibile classificare come locatori i fornitori da cui si ottengono gli elementi della configurazione in locazione e classificare come provider i fornitori che mettono a disposizione dei servizi.

I *fornitori* identificano le società che forniscono prodotti e servizi all'azienda, incluso il tipo di società e un contatto principale. Per fare riferimento a un fornitore, oltre agli elementi della configurazione è possibile utilizzare un record contatto dell'utente.

La definizione dei tipi di fornitore e dei fornitori consente di organizzare facilmente gli elementi della configurazione. Ad esempio, è possibile generare l'elenco di fornitori appartenenti a un determinato tipo e generare quindi l'elenco di elementi della configurazione in base a un fornitore specifico.

Elementi di configurazione

Gli *elementi della configurazione* sono i dispositivi, i componenti software e i servizi che costituiscono l'infrastruttura del business. Le informazioni associate a un elemento della configurazione identificano l'elemento della configurazione in modo univoco e ne indicano la posizione specifica. È possibile associare gli elementi della configurazione ai contatti (elementi della configurazione privati) e alle organizzazioni (elementi della configurazione condivisi). Gli elementi della configurazione consentono di identificare, visualizzare e specificare quanto segue:

- Identificare gli elementi della configurazione in base a nome, classe e famiglia.
- Specificare le informazioni di inventario.
- Specificare le proprietà aggiuntive per definire l'elemento della configurazione.
- Registrare e visualizzare i commenti associati all'elemento della configurazione.

- Specificare le informazioni sulla posizione dell'elemento della configurazione
- Specificare le informazioni sui servizi, ad esempio il tipo di servizio dell'elemento della configurazione.
- Visualizzare e definire i contatti e le organizzazioni assegnati all'elemento della configurazione
- Identificare le strutture gerarchiche e di pari livello (peer to peer) tra i vari elementi della configurazione
- Visualizzare i ticket associati all'elemento della configurazione

Non è necessario definire tutte queste informazioni per gli elementi della configurazione. Definendo tuttavia una quantità ottimale di informazioni per ciascun elemento della configurazione, si otterrà un quadro più chiaro durante l'analisi dell'impatto eseguita per l'organizzazione IT.

Ulteriori informazioni:

Creazione di un elemento della configurazione (a pagina 585)
Contatto, posizione ed elementi della configurazione dell'organizzazione (a pagina 588)
Relazioni elemento della configurazione (a pagina 592)

Strumenti di gestione degli asset esterni

È possibile integrare l'installazione di CA SDM con altri strumenti di gestione degli asset quali CA NSM, CA Asset Management e CA APM. Tra le funzioni di gestione degli asset di questi strumenti di CA SDM sono incluse le seguenti:

- CA NSM fornisce l'utilità pdm_nsmimp (solo per Windows) per l'aggiunta di informazioni sugli asset a CA SDM.
- CA Asset Management fornisce un set completo di funzioni hardware e software per l'inventario. Quando viene visualizzato un elemento della configurazione nel client CA SDM, è possibile fare clic sul pulsante Visualizzatore asset per visualizzare ulteriori informazioni rilevate sull'asset.

  L'integrazione tra CA SDM e CA Asset Management viene attivata quando i prodotti sono installati sullo stesso MDB.

- CA Asset Portfolio Management fornisce un set completo di funzioni relative al ciclo di vita dell'asset. Quando viene visualizzato un elemento della configurazione nel client CA SDM, è possibile fare clic sul pulsante Visualizzatore asset per visualizzare ulteriori informazioni finanziarie relative all'asset.

  L'integrazione tra CA SDM e CA Asset Portfolio Management viene attivata quando i prodotti sono installati sullo stesso MDB.

Nota: per ulteriori informazioni sull'integrazione dell'installazione di CA SDM con altri strumenti di gestione degli asset, consultare la *Guida all'implementazione*.

Multi-Tenancy

Con il termine *multi-tenancy* si intende la possibilità per più titolari indipendenti (e per i relativi utenti) di condividere una singola implementazione di CA SDM. Gli utenti titolari interagiscono solo nei modi specificati dai relativi *ruoli* e dalle relative *gerarchie di titolari.* In genere, a meno che non gli sia stato garantito l'accesso da un ruolo o da una gerarchia, ogni titolare visualizza l'implementazione di CA SDM esclusivamente per uso proprio e non può aggiornare o visualizzare i dati di un altro titolare.

La funzione multi-tenancy consente ai titolari di condividere le risorse di supporto hardware e software riducendo il costo di entrambe e ottenendo nel contempo gran parte dei vantaggi derivanti da un'implementazione indipendente.

Nota: per informazioni sull'installazione e sulla configurazione della funzione multi-tenancy, consultare la *Guida all'implementazione*.

Fornitore servizio

Il *fornitore del servizio* è il titolare primario (proprietario) in un'installazione multi-tenancy di CA SDM. Il primo titolare aggiunto ad un'installazione di CA SDM è sempre il titolare fornitore del servizio. Il titolare fornitore del servizio non può presentare un titolare padre.

CA SDM associa l'utente con privilegi (in genere ServiceDesk in Windows o srvcdesk in Linux/UNIX) al titolare fornitore del servizio.

Solo il titolare fornitore del servizio può eseguire le seguenti attività di CA SDM:

- Impostare le opzioni CA SDM
- Impostare le opzioni Gestione della conoscenza
- Impostare le opzioni Support Automation
- Creare tabelle o colonne

- Creare, modificare o eliminare titolari
- Consentire titolari secondari per i titolari
- Aggiornare i dati pubblici

  Nota: un amministratore può consentire l'accesso agli utenti titolari a dati di altri utenti. Gli analisti titolari non fornitore del servizio possono accedere solo ai relativi titolare e titolari secondari, a meno che il proprio accesso alle funzioni non venga aggiornato per includere il titolare dell'analista. In una definizione di ruolo può ad esempio essere impostato l'accesso separato in lettura e scrittura a determinati gruppi di titolari per gli utenti inclusi nel ruolo specifico.

Importante: il primo titolare creato viene impostato come fornitore del servizio. In seguito a questa operazione, la casella di controllo Fornitore del servizio e il campo Stato record sono di sola lettura.

Ulteriori informazioni:

Amministrazione del fornitore del servizio (a pagina 124)
Accesso titolare (a pagina 127)
Creazione di un titolare (a pagina 137)

Amministrazione del fornitore del servizio

Il fornitore del servizio può consentire ai titolari di amministrare le proprie impostazioni. Gli amministratori di titolari possono accedere ad un sottoinsieme di attività amministrative che sono identiche per tutti i titolari. La tabella ADMIN_TREE stessa non presenta pertanto titolari. Il ruolo Amministratore titolari definisce invece le funzioni di amministrazione disponibili per gli amministratori di titolari.

Per designare un utente come amministratore di titolari, selezionare Amministratore titolari come ruolo dell'utente.

Descrizione della funzione multi-tenancy

Quando è attiva la funzione multi-tenancy, è possibile concedere ad ogni contatto l'accesso a tutti i titolari (pubblico), a un singolo titolare o ad un gruppo di titolari (definito dall'utente o gestito dal prodotto). Il ruolo di un contatto controlla l'accesso che specifica indipendentemente l'accesso in lettura e scrittura. Poiché l'accesso titolare è dipendente dal ruolo e un contatto può cambiare ruoli durante una sessione, può cambiare anche l'accesso del titolare del contatto.

Se è installata la funzione multi-tenancy, la maggior parte degli oggetti CA SDM include un attributo titolare che specifica il titolare proprietario dell'oggetto. Gli oggetti rientrano in tre gruppi, in base al relativo attributo titolare e alla modalità di utilizzo di quest'ultimo:

Senza titolare

Definisce gli oggetti senza un attributo titolare. Tutti i dati presenti in questi oggetti sono pubblici.

Esempi: priorità e urgenza.

Titolare richiesto.

Definisce gli oggetti con un attributo titolare che non può essere null (applicato da CA SDM e non dal DBMS). Tutti i dati contenuti in questi oggetti sono associati a singoli titolari e non sono pubblici.

Esempi: tabelle Ticket (Richiesta, Issue e Ordine di cambiamento).

Titolare facoltativo

Definisce gli oggetti con un attributo titolare che può essere null. Alcuni dei dati di questi oggetti sono pubblici, altri sono associati a titolari specifici. La visualizzazione dell'oggetto di ogni titolare è una visualizzazione unita dei dati pubblici e dei relativi dati specifici del titolare.

Esempi: categoria e posizione.

Quando un utente esegue una query sul database, CA SDM limita i risultati agli oggetti appartenenti ai titolari per i quali l'utente dispone di accesso. Questa restrizione si applica in aggiunta a quelle relative alle partizioni di dati attive. Ciò significa che nelle tabelle dei titolari richiesti e facoltativi non saranno mai presenti dati diversi da quelli appartenenti ai titolari per i quali si dispone delle autorizzazioni di accesso.

Quando un utente chiede di creare o aggiornare un oggetto del database, CA SDM verifica che l'oggetto appartenga ad un titolare di cui è consentito l'aggiornamento dal ruolo corrente dell'utente e che tutti i riferimenti di chiave esterna (SREL) dell'oggetto ad altri oggetti siano ad oggetti pubblici (senza titolare), ad oggetti dello stesso titolare o ad oggetti dei titolari della gerarchia di titolari al di sopra del titolare dell'oggetto. In altre parole, a un oggetto titolare è consentito fare riferimento ad oggetti appartenenti al relativo titolare padre, al padre del relativo padre e così via.

Se un utente che crea un oggetto dispone di accesso in aggiornamento a più titolari, deve specificare il titolare in modo esplicito, direttamente o indirettamente.

Nota: esiste una sola eccezione alla restrizione relativa ai riferimenti SREL. Determinati riferimenti SREL, ad esempio l'assegnatario di un incidente, possono essere applicati ad oggetti che appartengono a titolari presenti nella gerarchia di titolari del relativo oggetto contenente. Questo tipo di riferimento è designato come SERVICE_PROVIDER_ELIGIBLE nello schema degli oggetti CA SDM (Majic). Il flag SERVICE_PROVIDER_ELIGIBLE fa la differenza solo se il titolare fornitore del servizio non si trova al di sopra del titolare dell'oggetto nella gerarchia di oggetti; se il titolare fornitore del servizio si trova nella gerarchia, le regole di convalida del titolare consentono riferimenti al fornitore del servizio.

Un utente fornitore del servizio che chiede la creazione o l'aggiornamento di un oggetto è soggetto alle stesse restrizioni degli utenti titolari, ad eccezione di quelli fornitori del servizio che possono essere autorizzati a creare o aggiornare oggetti pubblici. Questa autorizzazione è controllata dal ruolo attivo dell'utente fornitore del servizio.

Nota: se CA SDM impedisce ad un utente l'aggiornamento dei dati del titolare, un messaggio di errore può annunciare una limitazione relativa alle partizioni di dati. Se si riceve questo messaggio di errore, sono attive le restrizioni relative alle partizioni di dati o alla funzione multi-tenancy.

Opzione Multi-Tenancy

È possibile attivare multi-tenancy installando una delle seguenti opzioni multi-tenancy.

- **disattiva**—Multi-tenancy non è in uso. Le funzioni multi-tenancy non sono disponibili e gli oggetti non presentano un attributo titolare. Questa opzione è l'impostazione predefinita in una nuova installazione di CA SDM.
- **installazione**—le funzioni multi-tenancy sono attive per gli amministratori. Gli attributi e gli oggetti correlati al titolare sono pertanto visibili e modificabili. CA SDM non applica tuttavia restrizioni relative alla proprietà, pertanto gli utenti non amministrativi non saranno in grado di visualizzare le modifiche. Questa impostazione consente la preparazione di un amministratore al supporto multi-tenancy mediante l'esecuzione di attività quale la definizione dei titolari o l'assegnazione di oggetti ai titolari senza alcun impatto sul normale utilizzo di CA SDM.
- **attiva**—Multi-tenancy è completamente operativo. Tutti gli utenti possono visualizzare le modifiche all'interfaccia utente che li riguardano e CA SDM applica le restrizioni sulla proprietà.

Nota: per ulteriori informazioni sull'installazione e sull'implementazione della funzione multi-tenancy, incluse opzioni aggiuntive per la relativa applicazione, consultare la *Guida all'implementazione*.

Informazioni sul titolare

I titolari vengono creati e aggiornati quando si installa il supporto multi-tenancy (in modalità di installazione o di applicazione completa). Le informazioni gestite per un titolare sono simili ai dati gestiti per l'organizzazione, ad eccezione dei due seguenti attributi:

Logo

Fornisce un URL per un file di immagine con il logo del titolare. Il logo viene visualizzato sia nella pagina dei dettagli del titolare che in sostituzione del logo CA nei moduli Web visualizzati da un utente titolare o in cui è presente un oggetto associato al titolare.

Fornitore servizio

Indica se il titolare è il fornitore del servizio. Il titolare fornitore del servizio è sempre il primo titolare aggiunto. Quando l'amministratore aggiunge il primo titolare, si verifica quanto segue.

- Il primo titolare diventa fornitore del servizio. Non è possibile modificare questa designazione.
- L'utente con privilegi (di solito ServiceDesk) e tutti i contatti del sistema (come System_AHD_Generated) vengono impostati per appartenere al nuovo titolare fornitore del servizio

  Nota: l'utente di sistema "Amministratore" viene aggiunto solo in Windows e non gli viene assegnato un titolare. L'utente con privilegi deve assegnare un titolare all'utente Amministratore manualmente.

Accesso titolare

Il ruolo di un utente CA SDM gestisce sia l'autorizzazione all'accesso che l'interfaccia utente. Il set di ruoli disponibili per gli utenti dipende dal relativo tipo di accesso. La configurazione multi-tenancy consente di controllare il titolare o il gruppo di titolari cui un utente può accedere nell'ambito del ruolo.

Nella scheda Autorizzazione della pagina Dettagli ruolo sono presenti gli elenchi a discesa Accesso titolare e Accesso in scrittura titolare. Accesso titolare è un campo di sola visualizzazione mentre Accesso in scrittura titolare consente anche di eseguire operazioni di creazione e aggiornamento.

Ai ruoli è possibile assegnare le seguenti associazioni:

Uguale all'accesso titolare (solo per Accesso in scrittura titolare)

Imposta Accesso in scrittura titolare sullo stesso valore dell'impostazione Accesso titolare. Si tratta dell'impostazione predefinita di Accesso in scrittura titolare ed è valida solo per questo tipo di accesso.

Tutti i titolari

Rimuove le restrizioni relative ai titolari. CA SDM consente ad un utente con un ruolo provvisto di questo tipo di accesso di visualizzare qualsiasi oggetto del database (accesso in sola lettura) o di creare e aggiornare (accesso in scrittura) qualsiasi oggetto con titolare del database. Quando gli utenti con accesso Tutti i titolari creano un oggetto, CA SDM richiede che selezionino il titolare del nuovo oggetto.

Singolo titolare

Imposta l'accesso titolare di un ruolo su un titolare con nome. Quando questa opzione è selezionata, viene visualizzato un secondo campo sull'interfaccia utente Web che consente la selezione di un titolare specifico. CA SDM consente a un utente con questo tipo di accesso la visualizzazione (accesso in lettura) o la creazione e l'aggiornamento (accesso in scrittura) dei soli oggetti associati al titolare con nome. Questa selezione è valida per Accesso titolare o Accesso in scrittura titolare.

Gruppo titolari

Imposta l'accesso titolare di un ruolo su un gruppo di titolari definito dall'utente o gestito dal sistema. Quando questa opzione è selezionata, viene visualizzato un secondo campo sull'interfaccia utente Web che consente la selezione di un gruppo di titolari specifico. CA SDM consente a un utente con questo ruolo di visualizzare (accesso in lettura) o creare e aggiornare (accesso in scrittura) solo gli oggetti associati ad uno dei titolari del gruppo in questione. Quando un utente provvisto di accesso Gruppo titolari crea un oggetto, CA SDM richiede che selezioni il titolare del nuovo oggetto. Questa selezione è valida per Accesso titolare o Accesso in scrittura titolare.

Titolare del contatto

Imposta l'accesso titolare di un ruolo sul titolare del contatto che lo utilizza. CA SDM consente a un utente con un ruolo con questo tipo di accesso la visualizzazione (accesso in lettura) o la creazione e l'aggiornamento (accesso in scrittura) dei soli oggetti associati al relativo titolare. Questa selezione è valida per Accesso titolare o Accesso in scrittura titolare.

Gruppo titolare del contatto (solo per gli analisti)

Imposta l'accesso al ruolo di un analista sul gruppo di titolari con cui lavora, come specificato nel relativo record contatto. Se l'utente con ruolo non è analista, questa selezione ha gli stessi effetti di Titolare del contratto. Questa selezione è valida per Accesso titolare o Accesso in scrittura titolare.

Gruppo titolare secondario del contatto

Imposta l'accesso titolare di un ruolo sul gruppo di titolari secondari del contatto che lo utilizza. CA SDM consente a un utente con un ruolo con questo tipo di accesso la visualizzazione (accesso in lettura) o la creazione e l'aggiornamento (accesso in scrittura) dei soli oggetti associati al relativo gruppo di titolari secondari. Questa selezione è valida per Accesso titolare o Accesso in scrittura titolare.

Gruppo titolare principale del contatto

Imposta l'accesso titolare di un ruolo sul gruppo di titolari principali del contatto che lo utilizza. CA SDM consente a un utente con un ruolo con questo tipo di accesso la visualizzazione (accesso in lettura) o la creazione e l'aggiornamento (accesso in scrittura) dei soli oggetti associati al relativo gruppo di titolari principali. Questa selezione è valida per Accesso titolare o Accesso in scrittura titolare.

Gruppo titolare del contatto correlato

Imposta l'accesso titolare di un ruolo sul gruppo di titolari correlati del contatto che lo utilizza. CA SDM consente a un utente con un ruolo con questo tipo di accesso la visualizzazione (accesso in lettura) o la creazione e l'aggiornamento (accesso in scrittura) dei soli oggetti associati al relativo gruppo di titolari correlati. Questa selezione è valida per Accesso titolare o Accesso in scrittura titolare.

Tutti gli utenti possono visualizzare i dati pubblici, indipendentemente dai diritti di accesso del relativo ruolo corrente. La casella di controllo Aggiornare oggetti pubblici controlla se un utente fornitore del servizio con il relativo ruolo dispone dell'autorizzazione per la creazione o l'aggiornamento dei dati pubblici. Gli utenti titolari, ovvero che appartengono ad un titolare diverso dal fornitore del servizio, non possono aggiornare i dati pubblici indipendentemente dal relativo ruolo.

Ulteriori informazioni:

Modifica dell'accesso del titolare a un ruolo (a pagina 129)

Modifica dell'accesso del titolare a un ruolo

È possibile assegnare o modificare l'accesso del titolare ad un ruolo.

Per modificare l'accesso del titolare ad un ruolo

1. Accedere a Gestione ruoli e protezione, Gestione ruoli, Elenco ruoli.

   Viene visualizzato l'Elenco ruoli.

2. Fare clic su un ruolo.

   Viene visualizzata la pagina Dettagli ruolo.

3. Fare clic su Modifica.

   Viene visualizzata la pagina Aggiorna ruolo.

4. Selezionare le opzioni per Accesso titolare e Accesso in scrittura titolare.

   Nota: prestare attenzione nella selezione delle diverse opzioni di queste impostazioni.

5. Fare clic su Salva.

   Vengono salvate le opzioni di accesso titolare aggiornate per il ruolo.

Condizioni d'uso titolare

Nella pagina iniziale visualizzata all'accesso a CA SDM viene presentato all'utente finale l'accordo sulle condizioni d'uso. L'accordo indica all'utente l'uso corretto del prodotto. L'utente deve accettare le condizioni d'uso per poter proseguire con l'accesso a CA SDM. Le voci vengono scritte nel registro standard e nel registro eventi utente dopo il tentativo di accesso alla sessione.

È possibile effettuare le seguenti azioni in relazione alle condizioni d'uso:

- Creare, aggiornare ed eliminare un accordo sulle condizioni d'uso.
- Associare un accordo sulle condizioni d'uso a un titolare.

  Nota: occorre attivare la funzionalità multi-tenancy e configurare uno o più titolari prima di poter associare un accordo sulle condizioni d'uso a un titolare.

- Obbligare l'utente finale ad accettare l'accordo ad ogni accesso.
- Consentire all'utente finale di ignorare l'accordo iniziale presentando un accordo sulle condizioni d'uso vuoto.

Ulteriori informazioni:

Modalità di configurazione delle condizioni d'uso (a pagina 131)

Modalità di configurazione delle condizioni d'uso

Nella pagina iniziale visualizzata all'accesso a CA SDM viene presentato all'utente finale l'accordo sulle condizioni d'uso. L'accordo indica all'utente l'uso corretto del prodotto. L'utente deve accettare le condizioni d'uso per poter proseguire con l'accesso a CA SDM. Se l'utente finale seleziona Accetto, viene effettuato l'accesso al sistema e visualizzato il modulo principale. Se l'utente seleziona Rifiuto, viene nuovamente visualizzata la pagina di accesso. Le voci vengono scritte nel registro standard e nel registro eventi utente dopo il tentativo di accesso alla sessione.

In genere, l'accordo sulle condizioni d'uso viene configurato per ogni titolare di un contatto. Se il titolare di un contatto è configurato con un accordo sulle condizioni d'uso non attivo o le condizioni d'uso non sono configurate oppure se nella casella a discesa Condizioni d'uso è selezionato <vuoto>, viene visualizzato l'accordo sulle condizioni d'uso del padre del titolare o dell'entità superiore di due livelli del titolare e così via. Se non viene trovato un accordo sulle condizioni d'uso ad alcun livello, il sistema procede con l'accesso. Se si configura un titolare con un accordo sulle condizioni d'uso vuoto, il sistema procede con l'accesso e viene visualizzato il modulo principale.

È possibile configurare le condizioni d'uso come indicato di seguito:

1. Attivare l'opzione multi-tenancy.
2. Configurate uno o più titolari.
3. Definire un accordo sulle condizioni d'uso.
4. Aggiornare un titolare affinché utilizzi l'accordo sulle condizioni d'uso definito.

Nota: per informazioni dettagliate su creazione e modifica di accordi sulle condizioni d'uso, consultare la *Guida in linea*.

Impatto sull'interfaccia utente

L'installazione della funzione multi-tenancy determina la modifica dell'interfaccia utente, a seconda dell'autorizzazione e dell'accesso titolare associati al ruolo dell'utente. Le modifiche riguardano sia gli utenti titolari che quelli fornitori di servizi.

Utenti titolare

Se il ruolo di un utente è limitato ad un solo titolare e l'utente non è amministratore, è possibile sostituire un logo del titolare personalizzato con il logo di CA Technologies predefinito in tutte le pagine. Questa sostituzione varia a seconda che un logo sia definito o meno nella pagina dei dettagli del titolare essendo pertanto facoltativa per quest'ultimo.

L'unica modifica all'interfaccia utente per gli utenti titolari non amministrativi consiste nell'eliminazione per gli oggetti pubblici di voci di menu e pulsanti che consentono l'aggiornamento o la modifica (il pulsante Modifica o il pulsante Crea nuovo in una pagina di elenco), in quanto gli utenti titolari non sono autorizzati all'aggiornamento di un oggetto pubblico.

Amministratori titolare

Gli amministratori titolari dotati di accesso Singolo titolare che visualizzano oggetti facoltativi per i titolari rilevano un'ulteriore modifica all'interfaccia. Le pagine di elenco di questi oggetti includono automaticamente una colonna Pubblici che specifica se la riga di elenco contiene dati pubblici. Il primo elemento del filtro di ricerca è inoltre un elenco a discesa Dati pubblici che contiene le seguenti selezioni:

- Includi (selezione predefinita)
- Escludi
- Solo

Un amministratore titolare con accesso a più titolari può visualizzare una colonna Titolare nelle pagine di elenco di tutti gli oggetti con titolare. Questa colonna sostituisce la colonna Pubblici negli elenchi di tabelle con titolari facoltativi.

Utenti che possono visualizzare un gruppo di titolari

Se il ruolo di un utente consente l'accesso in visualizzazione a più titolari o un utente fornitore del servizio dispone dell'autorizzazione Aggiornare oggetti pubblici, i moduli di elenco di CA SDM cambiano come illustrato di seguito.

Oggetti senza titolare

Gli oggetti senza titolare contengono solo dati pubblici. A un utente fornitore del servizio è consentita la creazione o l'aggiornamento di un oggetto senza titolare solo se il relativo ruolo dispone dell'autorizzazione Aggiornare oggetti pubblici. In caso contrario, nell'interfaccia utente vengono eliminati i pulsanti e le voci di menu che consentono di eseguire operazioni di aggiornamento o modifica, quali il pulsante Modifica stesso o il pulsante Crea nuovo in una pagina di elenco. Gli utenti titolari non possono aggiornare gli oggetti pubblici. In una pagina di elenco relativa ad un oggetto senza titolare, per tali utenti non sarà pertanto mai disponibile un pulsante Modifica o Crea nuovo.

Oggetti che richiedono un titolare

Gli oggetti che richiedono un titolare contengono solo dati associati ad un determinato titolare. I moduli di elenco per questi oggetti includono automaticamente una colonna Titolare dopo l'ultima colonna di collegamento. Il filtro di ricerca contiene inoltre un selettore di titolare che consente all'utente di limitare un elenco ad un singolo titolare.

Oggetti con titolare facoltativo

Gli oggetti con titolare facoltativo contengono sia dati specifici del titolare sia dati pubblici. I moduli di elenco di questi oggetti elencano automaticamente una colonna Titolare (l'assenza di un titolare indica un oggetto pubblico). Il filtro di ricerca contiene inoltre sia un selettore del titolare che un elenco a discesa Dati pubblici (lo stesso visualizzato dagli amministratori titolari).

Nota: se le tabelle che richiedono un titolare contengono erroneamente dati senza titolare in un sistema multi-tenancy, in esse sarà presente un elenco a discesa Dati pubblici e verrà visualizzato il seguente messaggio: "AHD05358 nn oggetti attivi senza titolare xxx all'avvio di Service Desk".

Utenti che possono aggiornare più titolari

Se il ruolo dell'utente consente di accedere a più titolari o il ruolo utente di un fornitore del servizio dispone dell'autorizzazione Aggiornare oggetti pubblici, in genere nel caso di un analista che lavora per un fornitore del servizio, le pagine dei dettagli cambiano come illustrato di seguito.

Oggetti senza titolare

Gli oggetti senza titolare contengono solo dati pubblici. Non vengono apportate modifiche alle relative pagine dei dettagli per un utente fornitore del servizio provvisto dell'autorizzazione Aggiornare oggetti pubblici. Se l'utente presenta un ruolo sprovvisto dell'autorizzazione Aggiornare oggetti pubblici o non appartiene al fornitore del servizio, nelle pagine di sola lettura degli oggetti senza titolare non è presente il pulsante Modifica.

Oggetti esistenti che richiedono un titolare

Gli oggetti che richiedono un titolare contengono solo dati associati ad un determinato titolare. Nelle pagine dei dettagli degli oggetti esistenti che richiedono un titolare, il titolare dell'oggetto viene mostrato all'interno dell'intestazione di pagina standard.

Oggetti con titolare facoltativo

Gli oggetti con titolare facoltativo contengono sia dati specifici del titolare sia dati pubblici. La pagina dei dettagli di questi oggetti dipende dall'eventuale appartenenza dell'utente al fornitore del servizio e ad un ruolo provvisto dell'autorizzazione Aggiornare oggetti pubblici:

- Se il ruolo di un utente fornitore del servizio dispone dell'autorizzazione Aggiornare oggetti pubblici, la pagina dei dettagli è identica a quella degli oggetti che richiedono un titolare.
- Se il ruolo dell'utente non dispone di tale autorizzazione o l'utente non appartiene al fornitore del servizio, le pagine dei dettagli degli oggetti pubblici non contengono un pulsante Modifica. Le altre pagine dei dettagli sono identiche a quelle relative agli oggetti che richiedono un titolare.

Impatto su Automazione supporto

L'impatto dell'opzione multi-tenancy sull'ambiente di supporto dipende dalle restrizioni applicate a titolare e ruolo di utenti finali e analisti. Il fornitore del servizio gestisce le autorizzazioni in lettura/scrittura sia per i dati specifici di titolari che per quelli pubblici. Ad esempio, un analista può gestire sessioni di assistenza dalla coda pubblica e da una coda specifica per titolare, ma l'analista può solo utilizzare gli strumenti Assistenza in tempo reale attivati per ciascun titolare.

Per gli utenti finali con accesso a Automazione supporto, non configurare l'utente finale in modo che abbia accesso in scrittura a un titolare che non è un titolare secondario del titolare proprietario dell'utente finale, a meno che il gruppo chiave esterna venga modificato per includere il titolare proprietario. Se l'utente finale seleziona un titolare di accesso o è invitato tramite un ticket in un titolare che non soddisfa questo criterio, viene visualizzato un errore quando tenta di accedere al client dell'utente finale di Automazione supporto. Questa restrizione non si applica se il titolare proprietario dell'utente finale è il fornitore del servizio.

Per gli analisti con accesso a Automazione supporto, non configurare l'analista in modo che abbia accesso in scrittura a un titolare che non è un titolare secondario del titolare proprietario dell'analista, a meno che il gruppo chiave esterna venga modificato per includere il titolare proprietario. Se l'analista tenta di gestire un utente finale, oppure di invitare un utente finale da un ticket, in un titolare che non soddisfa questi criteri, viene visualizzato un errore.

Analisti e utenti finali senza accesso in lettura al rispettivo titolare non possono avviare il client Automazione supporto. In questo caso, per gli analisti viene visualizzato un messaggio di avviso in CA SDM, ad esempio dalla scheda Automazione supporto principale.

È possibile utilizzare i seguenti ruoli per gestire utenti di Automazione supporto:

Analista automazione supporto

Consente di fornire supporto agli utenti finali utilizzando Assistenza in tempo reale. Il fornitore del servizio stabilisce l'accesso ai titolari appropriati e può attivare gli strumenti Assistenza in tempo reale e l'accesso in lettura/scrittura ad attività automatiche.

Importante Se un analista non fornitore del servizio ha accesso in scrittura a un titolare padre, di pari livello o non correlato, è necessario aggiornare l'accesso alle funzioni per tale titolare. Analisti senza accesso in lettura al rispettivo titolare non possono avviare il client Analista automazione supporto e in CA SDM viene visualizzato un messaggio di avviso, ad esempio dalla scheda Automazione supporto principale o da un ticket.

Amministratore automazione supporto

Configura l'ambiente Automazione supporto per analisti e utenti finali. Il fornitore del servizio stabilisce l'accesso ai titolari e consente di visualizzare un elenco a discesa di titolari nei moduli Elenco e Dettagli. Questi moduli consentono di selezionare dati di titolari specifici oppure pubblici quando si cercano, creano e modificano dati di Automazione supporto in un ambiente multi-tenancy.

Nota: per oggetti quali code, livelli di riservatezza e chat predefinite il titolare è facoltativo.

Impatto su Gestione della conoscenza

L'impatto della funzione multi-tenancy sull'ambiente della conoscenza dipende dalle restrizioni relative al titolare applicate agli utenti:

Utenti titolare

Sostituisce il logo del titolare con l'impostazione predefinita, se il ruolo è limitato ad un singolo utente.

Amministratori titolare

Consente agli amministratori di visualizzare sia dati pubblici sia dati specifici del titolare. Le pagine di elenco di questi oggetti includono automaticamente una colonna Pubblici che specifica se la riga di elenco è pubblica.

Quando si cerca la conoscenza, il filtro contiene un elenco a discesa Dati pubblici in cui sono disponibili le selezioni Includi (selezione predefinita), Escludi e Solo.

Nota: il titolare è facoltativo per oggetti quali i modelli dei processi di approvazione, le categorie, i documenti, i file e i forum.

Documenti e categorie della conoscenza

Per i documenti e le categorie della conoscenza il titolare è facoltativo. Per gli oggetti pubblici che non richiedono necessariamente un titolare, tenere presente le seguenti informazioni:

- I documenti della conoscenza pubblici possono essere aggiunti solo al di sotto delle categorie della conoscenza pubbliche.
- Le categorie della conoscenza pubbliche possono essere aggiunte solo al di sotto delle categorie pubbliche.
- Le categorie di titolari possono essere aggiunte al di sotto delle categorie pubbliche e al di sotto delle categorie di un titolare.
- Solo i documenti dei titolari possono essere aggiunti al di sotto delle categorie di titolari.
- I documenti pubblici e con titolare possono essere aggiunti al di sotto delle categorie pubbliche.

Nota: la funzionalità della categoria Taglia/Copia/Incolla è consentita solo se fonte e destinazione hanno lo stesso titolare o se la destinazione è pubblica.

I repository non richiedono necessariamente un titolare. L'amministratore può pertanto creare diversi repository per diversi titolari.

Le immagini incorporate sono consentite solo se il documento e l'immagine sono impostati sullo stesso titolare. Non richiedono inoltre un titolare le cartelle di allegati, gli allegati e gli allegati a collegamenti di documenti.

Classificazione FAQ

Quando si visualizza la classificazione FAQ per gli utenti titolari, tenere presente le seguenti informazioni relative ai documenti pubblici:

- I documenti pubblici vengono visualizzati da un numero più ampio di destinatari rispetto agli utenti titolari.

  La classificazione FAQ dei documenti pubblici è superiore a quella di un documento specifico di un titolare.

- Ogni titolare presenta esigenze diverse. I modelli di utilizzo pertanto variano da titolare a titolare.

In Soluzioni principali nella pagina iniziale self-service di CA SDM vengono visualizzati i primi cinque documenti pubblici, nonché i primi cinque documenti di un titolare.

Per configurare Soluzioni principali è possibile accedere a Conoscenza, Indagine soluzione, Impostazioni FAQ nella scheda Amministrazione.

Knowledge Report Card

Scheda Report della conoscenza consente agli analisti e agli amministratori di visualizzare diverse metriche, quali la creazione, la pubblicazione, gli accessi e i voti dei documenti. Questo report ha una durata predeterminata e dipende dall'analista, dalla categoria e dall'organizzazione.

Quando si utilizza la scheda Report della conoscenza per fornire le informazioni su un ruolo con accesso Singolo titolare, i dati sono limitati dai criteri del titolare.

Modalità di utilizzo di multi-tenancy

Utilizzare le seguenti procedure per amministrare le funzioni multi-tenancy di CA SDM.

Visualizzazione dei titolari

È possibile visualizzare i titolari da qualsiasi Elenco titolari.

Nota: questa funzionalità è disponibile solo se è installata l'opzione multi-tenancy (in una modalità diversa da quella di installazione).

Per visualizzare un titolare

1. Nella scheda Amministrazione selezionare Gestione protezione e ruoli.
2. Fare clic su Titolari.

   Viene visualizzato l'Elenco titolari.
3. (Facoltativo) Selezionare un titolare dall'Elenco Titolari.

   Viene visualizzata la pagina Dettagli titolare.

Nota: gli Elenchi Titolari vengono visualizzati in pagine quali Dettagli gruppo titolari e Titolari interessati dall'elemento della configurazione.

Creazione di un titolare

È possibile utilizzare il prodotto per creare un titolare.

Per creare un titolare

1. Nella scheda Amministrazione, selezionare Gestione protezione e ruoli, Titolari.

   Viene visualizzata la pagina Elenco Titolari.

   Nota: l'opzione Gestione protezione e ruoli, Titolari è disponibile solo quando la funzione multi-tenancy è installata (in modalità di attivazione o in modalità di installazione).
2. Fare clic su Crea nuovo.

   Viene visualizzata la pagina Crea nuovo Titolare.
3. Completare i campi modificabili in base alle esigenze:

   Nome

   Visualizza il nome del titolare.

   Fornitore servizio

   Indica se un titolare è fornitore del servizio. Il primo titolare creato è sempre fornitore del servizio.

   Numero titolare

   (Solo scopo informativo) Visualizza il numero del titolare. Questo campo non viene utilizzato da CA SDM.

Stato record

Imposta il titolare sullo stato Attivo o Non attivo.

Titolare padre

Specifica un altro titolare al di sopra di quello in questione che diventa *titolare secondario* in una gerarchia di titolari.

Titolari secondari consentiti

Consente titolari secondari per il titolare. Il titolare non può modificare l'impostazione.

Livello titolare

(Solo scopo informativo) Indica il livello del titolare.

Gruppo Titolari principali

(Solo scopo informativo) Identifica il gruppo dei titolari gestiti dal sistema che contiene questo titolare e tutti quelli al di sopra nella gerarchia di titolari.

Gruppo Titolari secondari

(Solo scopo informativo) Identifica il gruppo dei titolari gestiti dal sistema che contiene questo titolare e tutti quelli al di sotto nella gerarchia di titolari.

Gruppo chiave esterna

(Solo scopo informativo) Identifica il gruppo di titolari gestiti dal sistema che contiene i titolari cui può fare riferimento una SREL nei dati che appartengono a questo titolare. Il gruppo di chiavi esterne è uguale al gruppo di titolari principali.

Gruppo titolare correlato

(Solo scopo informativo) Identifica il gruppo di titolari gestiti dal sistema che è composto dai gruppi di titolari principali e dai gruppi di titolari secondari del titolare.

Condizioni d'uso

Specifica le condizioni d'uso del titolare.

Logo

Specifa l'URL del file del logo del titolare che può essere qualsiasi tipo di immagine Web.

Ubicazione

Visualizza la pagina di ricerca della posizione.

Contatto

Visualizza la pagina di ricerca del contatto.

Nota: se non è associato alcun contatto al rispettivo titolare, i campi Indirizzo di posta elettronica e Indirizzo di posta elettronica cercapersone non sono attivi.

4. Fare clic su Salva.

   Viene creato il titolare.

5. Chiudere la finestra.
6. Fare clic con il pulsante destro del mouse sull'Elenco Titolari e scegliere Aggiorna.

   L'Elenco Titolari viene aggiornato e visualizza il titolare creato.

7. (Facoltativo) Per assegnare questo titolare ai gruppi di titolari definiti dall'utente, fare clic su Aggiorna gruppi di titolari nella scheda Gruppi titolari.

Modifica di un titolare

È possibile modificare un titolare dalla scheda Amministrazione.

Nota: questa funzionalità è disponibile solo se è installata l'opzione multi-tenancy (in una modalità diversa da quella di installazione).

Per modificare un titolare

1. Nella scheda Amministrazione selezionare Gestione protezione e ruoli.
2. Fare clic su Titolari.

   Viene visualizzato l'Elenco titolari.

3. Fare clic con il pulsante destro del mouse su un titolare, quindi scegliere Modifica.

   Viene visualizzata la pagina Aggiorna titolari.

   Nota: quando si modifica un titolare esistente, vengono visualizzate le schede Titolari secondari ed Elementi della configurazione.

4. Eseguire le necessarie modifiche e fare clic su Salva.
5. Chiudere la pagina Aggiorna titolari.

   Viene visualizzato l'Elenco titolari.

6. Fare clic con il pulsante destro del mouse e scegliere Aggiorna.

   Viene visualizzato l'Elenco Titolari aggiornato.

Gerarchie di titolari

Una *gerarchia di titolari* è un gruppo di titolari strutturato creato dal sistema o modificato quando si assegna a un titolare un *titolare padre*. Il titolare diventa un *titolare secondario* del titolare padre e degli eventuali titolari superiori ad esso nella gerarchia.

Nota: il fornitore del servizio può creare più gerarchie non correlate oppure nessuna gerarchia. Anche in un sistema con gerarchie di titolari, è possibile definire titolari autonomi.

Un titolare secondario rappresenta generalmente una divisione dei rispettivi *titolari principali*. Un titolare secondario può disporre di proprie regole e dati aziendali e i dati del titolare principale sono "inseriti" automaticamente nel titolare secondario in sola lettura.

CA SDM supporta gerarchie di titolari di profondità illimitata. Tuttavia, il *fornitore del servizio* può specificare un limite al numero totale di titolari e alla profondità delle gerarchie di titolari (l'impostazione predefinita è quattro livelli). Il fornitore del servizio può inoltre stabilire se singoli titolari possono avere titolari secondari.

Nota: il fornitore del servizio può partecipare alle gerarchie di titolari, ma non obbligatoriamente. Il fornitore del servizio non può avere un titolare padre.

Creazione di un titolare secondario

È possibile creare e modificare gerarchie di titolari a scopi organizzativi e di condivisione dei dati. Per inserire un titolare in una gerarchia di titolari, è necessario assegnarlo a un titolare padre.

Per creare un titolare secondario

1. Nella scheda Amministrazione, selezionare Gestione protezione e ruoli, Titolari.

   Viene visualizzato l'Elenco titolari.

   Nota: l'opzione Gestione protezione e ruoli, Titolari è disponibile solo se è attivata l'opzione multi-tenancy.

2. Fare clic su un titolare esistente da modificare oppure fare clic su Crea nuovo.

   Viene visualizzata la pagina Dettagli titolare. Immettere i dati o le modifiche desiderate.

3. Selezionare un titolare padre.

   Nota: nell'elenco a discesa dei titolari padre sono visualizzati solo i titolari che possono avere titolari secondari.

4. Fare clic su Salva.

   Il titolare è un titolare secondario del titolare padre selezionato.

   Nota: quando un titolare è un titolare secondario, appartiene al gruppo Titolari secondari del titolare padre, analogamente agli eventuali titolari secondari del titolare secondario, e così via. Il titolare padre appartiene al gruppo Titolari principali del titolare secondario, analogamente agli eventuali titolari principali del titolare principale, e così via. Ognuno appartiene al gruppo Titolari correlati dell'altro.

Gruppi di titolari gestiti dal sistema

CA SDM genera e gestisce automaticamente tre gruppi di titolari per ogni titolare di una gerarchia di titolari (*tenant* è il nome del titolare):

- *tenant*_subtenants (il titolare, i suoi titolari figlio e i loro titolari secondari nella gerarchia)
- *tenant*_supertenants (il titolare, il suo titolare padre e i loro titolari principali nella gerarchia)
- *tenant*_relatedtenants (l'intera singola gerarchia)

I gruppi di titolari gestiti dal sistema possono essere utilizzati come i gruppi di titolari definiti dall'utente. Tuttavia, è possibile modificarne solo il nome e la descrizione.

Visualizzazione dei gruppi di titolari

È possibile visualizzare le informazioni sui gruppi di titolari per mostrare i membri dei gruppi.

Nota: questa funzionalità è disponibile solo se è installata l'opzione multi-tenancy (in una modalità diversa da quella di installazione).

Per visualizzare l'Elenco Gruppi titolari

1. Nella scheda Amministrazione selezionare Gestione protezione e ruoli.

2. Fare clic su Gruppi titolari.

   Viene visualizzato l'Elenco Gruppi titolari.

   Nota: è possibile scegliere di visualizzare o nascondere i gruppi di titolari gestiti dal sistema.

3. (Facoltativo) Selezionare un gruppo di titolari dall'elenco.

   Vengono visualizzate le informazioni relative al gruppo di titolari.

4. Modificare il gruppo di titolari in base alle esigenze.

Creazione di un gruppo di titolari

È possibile utilizzare il prodotto per creare un gruppo di titolari.

Per creare un gruppo di titolari

1. Nella scheda Amministrazione selezionare Gestione protezione e ruoli.
2. Fare clic su Gruppi titolari.

   Viene visualizzato l'Elenco Gruppi titolari.

   Nota: l'opzione Gestione protezione e ruoli, Gruppi titolari è disponibile solo quando è installata la funzione multi-tenancy (in modalità di attivazione o in modalità di installazione).

3. Fare clic su Crea nuovo.

   Viene visualizzata la pagina Crea Nuovo gruppo titolari.

4. Inserire i dati nei seguenti campi:

   Nome gruppo titolare

   Visualizza il nome del gruppo di titolari.

   Stato record

   Imposta il gruppo di titolari come attivo o non attivo.

   Descrizione

   Visualizza una descrizione del gruppo di titolari.

5. Fare clic su Salva.

   Il gruppo di titolari viene creato.

6. Chiudere la finestra.

   Viene visualizzato l'Elenco Gruppi titolari.

7. Fare clic con il pulsante destro del mouse sull'Elenco Titolari e scegliere Aggiorna.

   L'Elenco Gruppi titolari viene aggiornato.

8. Fare clic su Aggiorna titolari nella pagina Dettagli gruppo titolari per aggiungere membri titolari al gruppo.

Modifica di un gruppo di titolari

È possibile modificare un gruppo di titolari per gestirne i membri e le informazioni dettagliate.

Nota: questa funzionalità è disponibile solo se è installata l'opzione multi-tenancy (in una modalità diversa da quella di installazione).

Per modificare un gruppo di titolari

1. Nella scheda Amministrazione selezionare Gestione protezione e ruoli.
2. Fare clic su Gruppi titolari.

   Viene visualizzato l'Elenco Gruppi titolari.
3. Fare clic con il pulsante destro del mouse su un gruppo di titolari, quindi scegliere Modifica.

   Viene visualizzata la pagina Aggiorna gruppo titolari.
4. Eseguire le necessarie modifiche e fare clic su Salva.
5. Chiudere la finestra.

   Viene visualizzato l'Elenco Gruppi titolari.
6. Fare clic con il pulsante destro del mouse nella finestra del registro e scegliere Aggiorna.

   Viene visualizzato l'Elenco Gruppo titolari aggiornato.

Assegnazioni di dati titolare

CA SDM visualizza il titolare nello stesso formato sia nelle versioni di visualizzazione che di modifica di una pagina dei dettagli per un oggetto esistente, in quanto il titolare di un oggetto esistente non può essere modificato dall'interfaccia Web.

Quando si modifica un oggetto con titolare, gli elenchi a discesa presenti nella pagina di modifica conterranno automaticamente solo i valori pubblici, di proprietà dello stesso titolare dell'oggetto di base o dei titolari al di sopra di esso nella gerarchia di titolari oppure di proprietà del fornitore del servizio (se l'elenco a discesa si applica ad un attributo SERVICE_PROVIDER_ELIGIBLE).

Non vengono apportate modifiche nella pagina dei dettagli ai campi di ricerca associati ad un oggetto con titolare. Se un utente con accesso a più titolari fa clic su un collegamento di ricerca ad una tabella con titolari, il motore Web limita automaticamente la ricerca ai valori appropriati per l'attributo, quindi visualizza un messaggio con intestazione nella pagina elenco o nella pagina di ricerca popup.

Nota: le restrizioni relative al titolare non vengono visualizzate nel filtro di ricerca e non possono essere modificate dall'utente.

Quando viene richiesta la creazione di un oggetto con titolare, il titolare diventa un selettore, ovvero un elenco a discesa o di ricerca.

Se il campo del titolare è vuoto, è possibile specificare un valore direttamente inserendolo nel campo o indirettamente indicando un valore per un attributo che implica la presenza di un titolare, ad esempio Utente finale interessato. Nell'interfaccia vengono visualizzati i seguenti suffissi:

(T)

Indica un attributo che implica la presenza di un titolare, ovvero una ricerca in una tabella con titolare obbligatorio.

(TO)

Indica un attributo che implica la presenza facoltativa di un titolare, ovvero una ricerca in una tabella con titolare facoltativo.

Il testo di questi indicatori è controllato dalle proprietà web.cfg.

Ad eccezione dell'attributo titolare stesso, gli attributi che implicano la presenza di un titolare vengono sempre visualizzati come ricerche, anche se creati con una macro dtlDropdown.

CA SDM imposta il titolare automaticamente quando viene cercato o immesso automaticamente un valore con titolare in un campo che implica la presenza di un titolare (ad eccezione di questo caso l'inserimento in un campo SERVICE_PROVIDER_ELIGIBLE di un riferimento ad un oggetto fornitore del servizio non determina l'impostazione del titolare). Una volta impostato il titolare, le ricerche dei campi che implicano la presenza di un titolare vengono limitate in modo analogo a quelle relative a oggetti con titolari esistenti.

Nota: il campo del titolare rimane modificabile fino a quando non si salva l'oggetto. Il titolare può essere modificato direttamente aggiornandolo. Quando si modifica il titolare, CA SDM cancella automaticamente i campi che implicano la presenza di un titolare contenente riferimenti ad oggetti appartenenti al titolare precedente.

In CA SDM il selettore Titolare viene avviato come vuoto. Questo comportamento può essere modificato in diversi modi:

- Aprire la pagina Crea Nuovo da una pagina, quale Profilo rapido, in cui viene automaticamente inserito il valore di un campo che implica la presenza di un titolare
- Impostare la preferenza utente Mantieni titolare

  Si tratta di un una nuova preferenza utente che inizializza il titolare di nuovi oggetti allo stesso titolare dell'ultima pagina dei dettagli visualizzata o aggiornata o nell'ultima restrizione del filtro di ricerca della pagina di elenco.

- Aprire la pagina con un URL che specifichi un titolare in modo esplicito

  Questo valore non viene fornito negli URL predefiniti, ma è disponibile per consentire ai siti la creazione di voci di menu o pulsanti che consentano la specifica un titolare.

Nota: se si creano elementi della configurazione da un altro prodotto CA Technologies (come CA APM) o dall'interfaccia della riga di comando, l'oggetto è pubblico.

Ulteriori informazioni:

Creazione di un oggetto con titolare (a pagina 145)

Creazione di un oggetto con titolare

Il fornitore del servizio può aggiungere dati specifici del titolare a oggetti, quali Issue, Richieste, Ordini di cambiamento e così via. È possibile aggiungere un titolare ad un ticket (ad esempio un Incidente) creato da una scheda Contatore.

Per aggiungere i dati del titolare a un Incidente

1. Fare clic su File, Nuovo Incidente.
2. Completare una delle seguenti procedure:
   a. Selezionare il titolare dall'elenco a discesa Titolare.
   b. Fare clic su Utente finale interessato (o su qualsiasi altro campo che implichi un titolare).

      Viene visualizzata la pagina Ricerca contatto. Cercare un utente: è possibile filtrare la ricerca in base al titolare.
   c. Immettere un nome nel campo Utente finale interessato.

      I dati del titolare vengono inseriti automaticamente.
3. Continuare a creare l'incidente.

Notifiche delle attività

Le notifiche attività controllano sia il contenuto delle notifiche sia i contatti che ricevono le notifiche dei vari eventi nella cronologia di un ticket.

In un ambiente multi-tenancy la regola di notifica è un oggetto per il quale il titolare è facoltativo. Le regole di notifica pubblica si applicano a tutti i ticket: le regole con titolare si applicano solo allo stesso titolare della regola o ai titolari nella relativa gerarchia di titolari secondari. La restrizione relativa al titolare viene applicata in aggiunta alle eventuali condizioni specificate con la regola stessa.

Ulteriori informazioni:

Copia delle regole di notifica (a pagina 146)

Copia delle regole di notifica

Le regole di notifica predefinite vengono memorizzate come oggetti pubblici. Se è installata la funzione multi-tenancy, è necessario creare una copia della regola di notifica per ogni titolare. In caso contrario, l'opzione Aggiorna contatti viene limitata.

Per copiare una regola di notifica

1. Accedere a Notifiche, Regole di notifica nella scheda Amministrazione.

   Viene visualizzato l'Elenco Regole di notifica.

2. Fare clic su una regola nella colonna Simbolo.

   Viene visualizzata la pagina Dettagli regola di notifica.

3. Fare clic su File, Copia.

   Riprendere l'aggiornamento della regola di notifica.

Repository

Per l'oggetto repository (doc_rep) il titolare è facoltativo. I titolari possono definire i propri repository. È possibile definire repository pubblici per oggetti quali gli allegati a documenti della conoscenza pubblici. Ogni titolare può presentare un repository predefinito ed è possibile specificare un repository pubblico predefinito.

Tutti gli allegati sono pubblici o associati ad un singolo titolare. Se un titolare non presenta un repository predefinito proprio, il repository pubblico viene visualizzato come predefinito per i relativi oggetti con titolare.

Capitolo 6: Integrazione di più motori di ricerca mediante la ricerca federata

La funzionalità di ricerca federata aumenta le capacità dell'archivio della conoscenza integrato di CA SDM.

- Quando un utente esegue una ricerca della conoscenza, i risultati dal database interno della conoscenza vengono ampliati con i risultati ottenuti nei motori di ricerca esterni. Il prodotto include una configurazione predefinita dell'adapter di ricerca per CA Open Space, Microsoft SharePoint e Google.
- L'architettura della ricerca federata è flessibile. Per includere il supporto di altri motori di ricerca è possibile creare un adapter di ricerca personalizzata tramite il Software Development Kit (SDK) per la ricerca federata di CA. L'interfaccia SDK presenta le informazioni e gli esempi di codice sorgente per l'estendibilità della ricerca federata.
- Inoltre, è possibile eseguire la ricerca nelle informazioni contenute nei ticket e negli articoli della conoscenza di CA SDM utilizzando un motore di ricerca esterno. Il nuovo componente di superficie crawler consente a un crawler del motore di ricerca esterno di rilevare facilmente le informazioni di CA SDM. Il crawler archivia queste informazioni nel repository corrispondente. È possibile cercare queste informazioni indicizzate utilizzando la ricerca federata. Sono supportati anche gli allegati di ticket e articoli della conoscenza.

I componenti principali della funzionalità di ricerca federata sono i seguenti:

- Configurazione della ricerca federata
- Configurazione del crawler
- Adapter di ricerca personalizzato di SDK

Configurazione della ricerca federata

La funzionalità di ricerca federata comprende i componenti seguenti:

Componenti di interfaccia utente

Consente agli utenti analisti di CA SDM di inserire argomenti di ricerca e trasferire la richiesta di ricerca al server di ricerca federata.

Servlet CAFedSearch

Componente principale della funzionalità di ricerca federata che utilizza un'interfaccia REST. Il servlet di ricerca federata viene eseguito su un'istanza di Tomcat dedicata all'interno dell'applicazione di CA SDM.

Adapter di ricerca plug-in

L'adapter di ricerca plug-in collega l'applicazione CA SDM a un motore di ricerca esterno. L'adapter converte le richieste di ricerca generiche in un formato proprietario del motore di ricerca e chiama il motore di ricerca. Il servlet di ricerca federata restituisce i risultati del motore di ricerca configurato al componente dell'interfaccia utente di CA SDM.

Il diagramma seguente mostra la procedura di configurazione della ricerca federata con l'applicazione CA SDM:

Procedere come descritto di seguito:

1. Completamento dei prerequisiti (a pagina 149)
2. Abilitazione della ricerca federata (a pagina 150)
3. Configurazione del file dell'utilità di ricerca federata (a pagina 150)
4. Creazione delle origini di ricerca federata in CA SDM (a pagina 157)

Completamento dei prerequisiti

Completare i seguenti prerequisiti:

- Verificare di aver selezionato l'opzione Ricerca federata nella procedura guidata Configura ricerca federata durante l'installazione dell'applicazione CA SDM.
- Definire i motori di ricerca da utilizzare nella ricerca federata.
- È necessario disporre di un account Google attivo per configurare l'adapter di ricerca del plug-in di Google. Inoltre sono richiesti una chiave API di Google e un ID del motore di ricerca personalizzato di Google. Per ulteriori informazioni, consultare la sezione Motore di ricerca personalizzato di Google all'indirizzo https://www.google.com/cse/all
- Verificare che il servizio IIS sul server SharePoint sia stato configurato con l'autenticazione di base. L'adapter di Microsoft SharePoint richiede l'autenticazione di base. Per impostazione predefinita, l'autenticazione di base è disabilitata in SharePoint. Per ulteriori informazioni sull'abilitazione dell'autenticazione di base in SharePoint, consultare la documentazione di Microsoft SharePoint.

  Nota: Abilitare l'autenticazione di base per _vti_bin in IIS.
- Per l'integrazione in CA Open Space, è richiesta la versione 2.0 SP1 della soluzione On Premise. Per ulteriori informazioni, consultare la documentazione di CA Open Space. L'offerta SaaS di CA Open Space non è attualmente supportata.

Abilitazione della ricerca federata

Un'istanza di Tomcat dedicata viene installata per ospitare i servlet CAFedSearch e FSCrawl. L'istanza Tomcat per la ricerca federata è controllata dalla gestione dei daemon. Tomcat viene avviato e arrestato in automatico all'avvio o all'arresto di CA SDM, rispettivamente.

Configurare il server Tomcat di ricerca federata (Federated Search, FS) con le seguenti opzioni di installazione:

Configurazione della ricerca federata

Verificare di aver selezionato questa opzione durante l'installazione dell'applicazione di CA SDM. Le opzioni Tomcat sono disponibili solo dopo aver selezionato questa opzione.

Porta Tomcat

Specifica la porta Tomcat della ricerca federata. Porta predefinita= 8040.

Porta di arresto Tomcat

Specifica la porta di arresto Tomcat della ricerca federata. Porta predefinita= 8045.

Generazione dei file XML di configurazione per la ricerca federata

Per configurare la ricerca federata e ridurre errori in fase di modifica, viene fornito il file dell'utilità fs_adapters_cli. Viene inoltre fornito un file per Windows e uno script shell per Linux e Unix. Il file dell'utilità è un'applicazione Java contenuta in due file JAR.

Vengono forniti tre file modello per gli adapter di CA Open Space, Google e SharePoint. Il file adapters-config.xml viene utilizzato per l'input e l'output nell'utilità. Il file adapters.properties viene utilizzato per l'input nell'utilità. Questo file contiene tutti i parametri di configurazione necessari per gli adapter. Il file jfedsearch.log contiene le informazioni del file di registro.

L'utilità fs_adapters_cli viene utilizzata per configurare il file adapters-config.xml. Il file dell'utilità consente di installare e disinstallare gli adapter mediante l'aggiunta o la rimozione di voci nel file adapters-config.xml. Vengono generati i singoli file di configurazione XML dell'adapter. Questi file vengono così inclusi in adapters-config.xml con la direttiva bean di <import>. Verificare di aver conservato una copia pulita di adapters-config.xml.

- Per installare un adapter, sono state aggiunte due voci per la registrazione e l'importazione dell'adapter nel file adapters-config.xml.
- Per disinstallare un adapter, vengono rimosse due voci per la registrazione e l'importazione dell'adapter dal file adapters-config.xml.

Per ulteriori informazioni sull'uso del file dell'utilità, consultare le sezioni File dell'utilità di ricerca federata e Attivazione del file dell'utilità per configurare gli adapter di ricerca.

File dell'utilità di ricerca federata

Il file dell'utilità fs_adapters_cli si trova nella directory $NX_ROOT\samples\cafedsearch di CA SDM. In questa posizione sono disponibili i componenti di file dell'utilità seguenti:

- File script:
  - fs_adapters_cli.bat (per ambienti Windows)
  - fs_adapters_cli.sh (per ambienti non Windows)
- File JAR:
  - fs_adapters_config_cli.jar
  - fs_adapters_config_schema.jar
- Modelli:
  - openspace-tmpl.xml
  - google-tmpl.xml
  - sharepoint-tmpl.xml
- Proprietà:
  - adapters.properties

Per installare il file dell'utilità di ricerca federata, immettere il comando seguente:

```
fs_adapters_cli -i -k <key> -b <bean> -t <filename> -p <filename> -o <filename>
[-c <filename>]
```

Utilizzare l'opzione fs_adapters_cli -h per visualizzare la guida in linea del file dell'utilità. Sono disponibili le seguenti opzioni di attributo:

-b (Facoltativo)

Valore dell'attributo per eseguire il mapping degli adapter. Fa riferimento a un ID effettivo di un bean dell'adapter. Se non è specificato, come valore per -b viene assunto il valore dall'opzione -k.

-c (Facoltativo)

Il file XML principale che contiene tutti gli adapter configurati.

-h (Facoltativo)

Visualizza la guida in linea per l'utilità di ricerca federata.

-i

Specifica l'opzione utilizzata per installare l'adapter.

-k

Specifica l'attributo di chiave dell'adapter.

-o

Specifica il nome del file XML di output da generare. Assegnare un nome al file XML da creare e aggiornare il contenuto unito del modello XML e del file di proprietà di SharePoint.

-p (Facoltativo)

Indica il nome del file di proprietà da unire al modello XML di definizione dell'adapter.

-t

Specifica il nome del file modello XML per definire un adapter.

-u

Specifica il nome del file XML per disinstallare l'adapter.

Attivazione del file dell'utilità per configurare gli adapter di ricerca

Un motore di ricerca richiede adapter plug-in appositamente codificati. Un adapter di ricerca plug-in converte le richieste di ricerca generiche in un formato proprietario del motore di ricerca, richiama il motore di ricerca e restituisce le richieste di ricerca.

Nota: Se CA SDM è configurato per la multi-tenancy, il titolare dell'utente viene comunicato al motore di ricerca. La ricerca federata prevede il supporto incorporato della multi-tenancy. È possibile utilizzarlo per isolare i dati di un titolare in un'implementazione singola di SharePoint.

Importante. Non utilizzare il simbolo di E commerciale o spazi nei valori del file adapters.properties.

Procedere come descritto di seguito:

1. Crittografare la password per gli adapter di ricerca utilizzando l'utilità encrypt_password. Per crittografare le password, accedere alla seguente directory di CA SDM:

   ```
   $NXROOT\bin
   ```

2. Eseguire il comando seguente per generare password crittografate:

   ```
   encrypt_pwd [-e] <search engine password>
   ```

   L'opzione predefinita è -e.

3. Aprire il file adapters.properties dalla seguente directory di CA SDM:

   ```
   $NX_ROOT\samples\cafedsearch
   ```

4. Modificare il file adapters.properties. Specificare i parametri appropriati per gli adapter da configurare.

5. Per SharePoint, aggiornare i valori seguenti nel file adapters.properties:

   sharepoint_username=

   Immettere il nome utente per l'accesso a SharePoint.

   sharepoint_password=

   Immettere la password crittografata per l'accesso a SharePoint come illustrato nella Fase1.

   sharepoint_hostname=

   Immettere il nome host.

   sharepoint_domainName=

   Immettere il nome del dominio.

   sharepoint_protocol=

   Immettere il protocollo di comunicazione (http o https)

   sharepoint_portNumber=

Immettere il numero di porta. Il valore predefinito è 80.

6. Per Google, aggiornare i valori seguenti nel file adapters.properties:

   google_googleCx=

   Immettere un valore di chiave univoco usato da Google per decidere quale account di ricerca personalizzata Google utilizzare.

   google_googleApiKey=

   Immettere il valore di chiave univoco in modo che Google possa determinare l'identità di un'applicazione. Per recuperare la chiave nella Console delle API, attivare l'API di ricerca personalizzata JSON/Atom. Quest'API fornisce una nuova chiave API per l'accesso API semplice.

7. Per CA Open Space, aggiornare i valori seguenti nel file adapters.properties:

   openspace_protocol=

   Immettere il protocollo di comunicazione (http o https)

   openspace_portNumber=

   Immettere il numero di porta per CA Open Space. Il valore predefinito è 8686.

   openspace_default_tenant_userName=

   Se CA SDM non è configurato con multi-tenancy, immettere un nome utente per eseguire la ricerca in CA Open Space.

   openspace_default_tenant_password=

   Immettere la password crittografata di CA Open Space. Per ulteriori informazioni, vedere la Fase1.

   openspace_default_tenant_companyHost=

   Immettere i dettagli host dell'azienda titolare.

a. In caso di multi-tenancy di CA SDM, aggiungere una voce per ciascun titolare in openspace-tmpl.xml:

Ad esempio, se CA SDM contiene il nome del titolare come Titolare 1, è necessario fornire i seguenti valori nel file openspace-tmpl.xml:

```
<entry key="Tenant1">
 <bean
class="com.ca.ServicePlus.cafedsearch.adapters.openspace.OpenSpaceCompanyDetail">
  <property name="userName"
value="$(openspace_tenant1_userName)"/>
   <property name="password"
value="$(openspace_tenant1_password)"/>
  <property name="companyHost"
value="$(openspace_tenant1_companyHost)"/>
  </bean>
</entry>
```

b. Aggiungere le voci seguenti per Titolare 1 nel file adapters.properties:

```
openspace_tenant1_userName=
openspace_tenant1_password=
openspace_tenant1_companyHost=
```

Ripetere i passaggi a e b per tutti i titolari obbligatori nel file openspace-tmpl.xml.

8. Richiamare fs_adapters_cli una volta per ciascun adapter da configurare.

■ Se si desidera configurare un adapter CA Open Space, utilizzare il valore bean OpenSpaceSearchAdapter e il modello openspace-tmpl.xml come illustrato nell'esempio seguente:

```
fs_adapters_cli -i -k OpenSpace -b OpenSpaceSearchAdapter -t "openspace-tmpl.xml" -o "openspace.xml"
```

■ Per configurare un adapter Google, fornire il valore bean GoogleSearchAdapter e il modello google-tmpl.xml come illustrato nell'esempio seguente:

```
fs_adapters_cli -i -k Google -b GoogleSearchAdapter -t "google-tmpl.xml" -o "google.xml"
```

■ Se si desidera configurare un adapter SharePoint, utilizzare il valore bean SharePointSearchAdapter e il modello sharepoint-tmpl.xml come illustrato nell'esempio seguente:

```
fs_adapters_cli -i -k SharePoint -b SharePointSearchAdapter -t "sharepoint-tmpl.xml" -o "sharepoint.xml"
```

Modificare i valori di attributo -k e -o con un nome desiderato. Per ulteriori informazioni sugli attributi e sul file dell'utilità di ricerca federata, consultare la sezione File dell'utilità di ricerca federata.

9. Dopo l'installazione, in caso di errori, controllare il file di registro presente nella directory di CA SDM:
   `$NXROOT\log\jfedsearch.log`

10. Se lo si desidera, è possibile creare il proprio file XML per la registrazione. Tutte le voci dell'adapter vengono registrate nel file adapters-config.xml disponibile nella directory seguente:

    ```
    $NX_ROOT\samples\cafedsearch
    ```

11. Per creare il proprio file XML per la registrazione, è possibile anche copiare il nome del file adapters-config.xml esistente (fase facoltativa). Assegnare al file adapters-config.xml modificato il nome desiderato. Ad esempio, file xyz.xml.

    Utilizzare l'opzione -c con il file XML modificato (xyz.xml) per la registrazione degli adapter.

12. Modificare il valore di risorsa in bean.xml <import resource="adapters-config.xml"/>.

13. Copiare il file adapters-config.xml o il file xyz.xml modificato (fase 11) e qualsiasi file XML associato e specifico di un adapter per Google (google.xml), CA Open Space (openspace.xml), SharePoint (sharepoint.xml) nella seguente directory di CA SDM:

    ```
    $NX_ROOT\bopcfg\www\CATALINA_BASE_FS\webapps\cafedsearch\WEB-INF
    ```

14. Riavviare l'istanza Tomcat di ricerca federata.

    ```
    pdm_tomcat_nxd –c STOP –t FS
    ```

    ```
    pdm_tomcat_nxd –c START –t FS
    ```

    La configurazione degli adapter di ricerca viene completata.

15. Consultare i file di registro degli errori nella directory di CA SDM:

    ```
    $NX_ROOT\log\jfedsearch.log
    ```

Creazione delle origini di ricerca federata in CA SDM

L'interfaccia utente Web di CA SDM viene associata in modo poco rigoroso al servlet CAFedSearch. Configurare le origini di ricerca in CA SDM per creare un nuovo record.

Procedere come descritto di seguito:

1. Accedere all'applicazione di CA SDM come amministratore Service Desk.
2. Selezionare Amministrazione, Conoscenza, Ricerca federata, Origini di ricerca per creare un nuovo record che rappresenta un motore di ricerca federata.

   L'origine di ricerca contiene il nome dell'origine di ricerca federata visualizzato.

   Nota: Il valore di codice deve corrispondere all'attributo di valore chiave di una voce nel file adapters-config.xml.

Ricerca nella soluzione della conoscenza mediante il nuovo adatper di ricerca personalizzato

Cercare documenti e articoli della conoscenza nell'applicazione di CA SDM mediante il nuovo adatper di ricerca personalizzato.

Procedere come descritto di seguito:

1. Accedere come amministratore Service Desk di CA SDM.
2. Accedere ad Amministrazione, Conoscenza, Ricerca federata, Origini di ricerca.
3. Aggiungere un valore chiave di codice per la nuova origine di ricerca.
4. Fare clic su Salva.
5. Accedere alla Gestione della conoscenza mediante un ticket nuovo o esistente.
6. Eseguire una ricerca all'interno della fonte della conoscenza di propria creazione. Fare clic su Mostra filtro per immettere i criteri di ricerca e fare clic su Cerca.

   Sono visualizzate le informazioni di ricerca.

Disinstallazione dell'adapter di ricerca

Per disinstallare gli adapter di ricerca, utilizzare il comando dell'utilità fs_search_cli con l'opzione -u. Utilizzare il seguente comando di file dell'utilità:

```
fs_adapters_cli -u -k <key> -b <bean> [-c <filename>]-f <filename>]
```

-u

Specifica l'opzione -u per disinstallare gli adapter di ricerca.

-k

Specifica il valore di nome della chiave fornito in fase di installazione.

-b

Specifica il valore bean fornito in fase di installazione.

-c

Specifica il nome del file XML di configurazione per il nuovo adapter di ricerca, se è stato creato durante la configurazione degli adapter di ricerca con l'utilità.

-f

Restituisce il nome del file di output generato in fase di installazione.

Per ulteriori informazioni, consultare la sezione Configurazione degli adapter con l'utilità.

Ad esempio, se si desidera disinstallare l'adapter di ricerca di Google, procedere come descritto di seguito:

Procedere come descritto di seguito:

1. Eseguire il comando di file dell'utilità con l'opzione -u per disinstallare l'adapter di ricerca di Google:

   ```
   fs_adapters_cli -u -k Google-b GoogleAdapter-f Google.xml
   ```

2. Verificare che la registrazione per Google sia rimossa da adapters-config.xml.
3. Il file Google.xml viene eliminato dalla seguente directory di CA SDM:

   ```
   $NX_ROOT\samples\cafedsearch
   ```

4. Copiare il file adapters-config.xml nella directory seguente:

   ```
   $NX_ROOT\samples\cafedsearch\WEB-INF
   ```

   Eliminare il file google.xml da questa posizione.

5. Riavviare Tomcat FS.

   ```
   pdm_tomcat_nxd –c STOP –t FS
   ```

   ```
   pdm_tomcat_nxd –c START –t FS
   ```

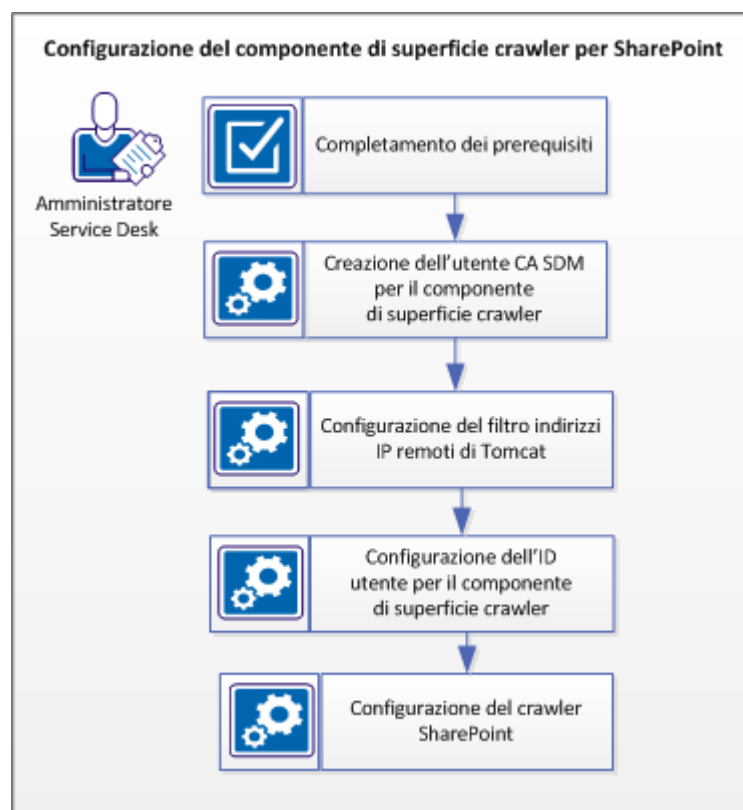
6. Nell'interfaccia utente di CA SDM, verificare la voce per l'attivazione dell'origine di ricerca per questo adapter (Google in questo caso).

7. Per disinstallare altri adapter di ricerca esterni, ripetere i passaggi da 1 a 6.

Configurazione della superficie crawler

Un crawler è un componente del motore di ricerca che esplora automaticamente Internet per indicizzare i termini di ricerca. La superficie crawler è una nuova interfaccia basata su Web di sola lettura dell'applicazione di CA Service Desk Manager. Il motore di ricerca esterno può rilevare le informazioni mediante la tecnologia Java Server Page (JSP). La superficie crawler fornisce le informazioni in testo non crittografato e anche i singoli collegamenti ipertestuali a ticket e documenti della conoscenza. Seguire i collegamenti ipertestuali per visualizzare i dettagli delle informazioni. È possibile utilizzare Microsoft SharePoint 2010 e SharePoint 2013 per effettuare una ricerca per indicizzazione nella superficie crawler. Il componente principale della superficie crawler è il servlet FSCrawl.

Nota: Il contenuto delle informazioni di CA Service Desk Manager mostrato a un crawler è personalizzabile tramite il file di configurazione. Non sono richieste modifiche al modulo.

Il diagramma seguente mostra la procedura per configurare la superficie Web crawler per SharePoint:

Procedere come descritto di seguito:

1. Completamento dei prerequisiti (a pagina 160)
2. Creazione della superficie crawler dell'utente di CA Service Desk Manager (a pagina 160)
3. Configurazione del filtro indirizzi IP remoti di Tomcat (a pagina 161)
4. Configurazione dell'ID utente della superficie crawler (a pagina 163)
5. Configurazione del crawler SharePoint (a pagina 170)

Completamento dei prerequisiti

Completare i prerequisiti seguenti prima di iniziare la configurazione della superficie crawler per un server di Microsoft SharePoint:

- Abilitare l'opzione Configura ricerca federata durante l'installazione dell'applicazione di CA SDM.
- Disporre di un ID utente dedicato per accedere alle informazioni dei risultati di ricerca. L'ID utente controlla le informazioni presenti nella superficie crawler. Per la configurazione multi-tenancy di CA SDM, creare ID utente aggiuntivi per permettere la separazione delle informazioni sul titolare.

Creazione della superficie crawler dell'utente di CA SDM

In una configurazione CA SDM, creare le identità utente per separare le informazioni in base al titolare.

Il processo di creazione di un ID utente per la superficie crawler coincide con la creazione delle identità utente di CA SDM per gli utenti ordinari. Creare un contatto con tipo di accesso e ruolo crawler nell'applicazione di CA SDM. Per ulteriori informazioni sulla creazione di un contatto, consultare la Guida in linea per l'amministratore di CA Service Desk Manager.

Il tipo di accesso e il ruolo crawler consentono all'utente un accesso in sola lettura ai dati di CA SDM.

Configurazione del filtro indirizzi IP remoti di Tomcat

Cambiare l'impostazione del filtro indirizzi IP remoti Tomcat affinché punti al sistema remoto che ospita il server di SharePoint. Sono supportati gli indirizzi IPV4 e IPV6.

La superficie crawler utilizza il meccanismo di filtro degli indirizzi IP remoti di Tomcat per accedere alle informazioni di CA SDM. Il meccanismo del filtro di Tomcat utilizza un modello di indirizzo IP (gestito dall'amministratore di CA SDM) per stabilire la corrispondenza con gli indirizzi IP autorizzati. Per impostazione predefinita, il filtro degli indirizzi IP remoti è configurato con l'indirizzo IP dell'adapter di loopback 127.0.0.1. In un ambiente di produzione, ai fini della comunicazione protetta, valutare l'utilizzo di SSL tra il crawler e la superficie crawler.

Procedere come descritto di seguito:

1. Accedere al server seguente, a seconda della configurazione di CA SDM:
   - Convenzionale: server primario o secondario
   - Disponibilità avanzata: server applicazioni
2. Aprire il file web.xml dalla seguente directory di CA SDM:

   ```
   $NX_ROOT\bopcfg\www\CATALINA_BASE_FS\webapps\fscrawl\WEB-INF
   ```
3. Creare una copia di backup del file web.xml.
4. Trovare la sezione <filter-name>Remote Address Filter</filter-name>. Modificare il modello in <param-value> nel <filter>.

   Questo parametro consente di specificare un intervallo di modelli indirizzo IP. Fornire inoltre l'accesso dal computer remoto che ospita SharePoint. Per ulteriori informazioni sul filtro indirizzi IP remoti di Tomcat, consultare la Documentazione di Apache Tomcat.
5. Salvare il file XML.
6. Riavviare il server Tomcat della ricerca federata.

   Nota: Quando si riavvia il server Tomcat della ricerca federata, gli utenti non possono eseguire alcuna ricerca federata.
7. Il valore del filtro indirizzi IP remoti di Tomcat viene cambiato ed è possibile accedere alla superficie crawler dal computer remoto.

   Nota: Non accedere alla superficie crawler da un indirizzo IP non configurato. L'utente viene reindirizzato all'interfaccia utente di CA SDM.
8. La superficie crawler è accessibile tramite un URL come qualsiasi altra applicazione Web. Per convalidare l'accesso con SharePoint, immettere l'URL seguente in un browser:

   ```
   http://<sdmhostname>:<FS_TOMCAT_PORT>/fscrawl/index.jsp?farm=<FarmName>
   ```

   Nota: Tutti gli elementi dell'URL rispettano la distinzione tra maiuscole e minuscole.

   nome host

Specifica il nome di dominio completo al server Tomcat di ricerca federata

port number

Definisce il numero di porta predefinito assegnato al server Tomcat di ricerca federata durante l'installazione e la configurazione dell'applicazione CA SDM. Viene utilizzato per accedere a Tomcat di ricerca federata.

fscrawl

Specifica il nome del servlet. I nomi di servlet rispettano la distinzione tra maiuscole e minuscole. Specificare sempre fscrawl.

index.jsp

Specifica il nome della pagina utilizzabile per provare la configurazione della superficie crawler.

<FarmName>

Ogni <farm> in crawler_surface_config.xml contiene la voce di <sdm_user>. Deve corrispondere all'utente autenticato. Le richieste vengono reindirizzate all'interfaccia utente Web di CA SDM in caso di autenticazione utente non riuscita. <sdm_user> controlla l'accesso ai dati a livello della gestione oggetto di CA SDM. Questo livello di protezione su <farm> impedisce a un titolare di accedere ai dati di un altro titolare.

Configurazione dell'ID utente della superficie crawler

Configurare l'ID utente della superficie crawler nel file crawler_surface_config.xml per modificare la superficie crawler.

Importante. È necessario che siano note le impostazioni linguistiche del browser. La risposta di SharePoint varia a seconda della lingua utilizzata nella richiesta di ricerca.

Procedere come descritto di seguito:

1. Accedere al seguente server di CA SDM che ospita la superficie crawler a seconda della configurazione di installazione:
   - Convenzionale: server primario o secondario
   - Disponibilità avanzata: server applicazioni
2. Aprire il file crawler_surface_config.xml dalla seguente directory di CA SDM:

   `$NX_ROOT\bopcfg\www\CATALINA_BASE_FS\webapps\fscrawl\WEB-INF`
3. Eseguire il backup del file crawler_surface_config.xml.

   Importante. Apportare tutte le modifiche al file XML in un ambiente di test prima di inserire le modifiche finali in un server di produzione.
4. Nel file originale, individuare *<sdm_user>CHANGE_THIS</sdm_user>* in ciascuna sezione *<farm>* e sostituire *CHANGE_THIS* con l'ID utente del crawler creato in precedenza.
5. È possibile modificare ulteriormente e limitare gli attributi di oggetto XML a seconda dei requisiti.

   Nota: Per ulteriori informazioni, consultare la sezione File di configurazione XML della superficie crawler.
6. Salvare il file XML.
7. Riavviare il server Tomcat della ricerca federata per ricaricare il file.

   Il file XML della superficie crawler è modificato.

File di configurazione XML della superficie crawler

Il file crawler_surface_config.xml contiene le seguenti sezioni XML.

<objects>

Specifica le informazioni sugli oggetti e sugli attributi visualizzati dalla superficie crawler per un oggetto. La sezione oggetti descrive il layout di una pagina dei dettagli per ciascun tipo di oggetto che viene visualizzato a un crawler. Questa sezione non controlla la selezione dei singoli record. La sezione <objects> è una raccolta di sezioni informazioni di accesso.

Ciascun oggetto è definito in una sezione informazioni di accesso. Le specifiche predefinite fornite per questi oggetti sono:

DC

Specifica i documenti della conoscenza.

chg

Specifica gli Ordini di cambiamento.

iss

Specifica le Issue.

in

Specifica gli Incidenti.

pr

Specifica i Problemi.

cr

Specifica le Richieste.

Il file XML contiene le sezioni seguenti che creano la sezione <head> di una pagina dei dettagli in CA SDM:

<name>

Specifica il nome oggetto Majic dell'oggetto visualizzato.

<note>

Specifica lo spazio in cui inserire una breve descrizione dell'oggetto. Questo elemento esiste solo ai fini della documentazione e viene ignorato dalla superficie crawler.

<last_mod_dt>

Specifica il nome dell'attributo che archivia la data e l'ora dell'ultima modifica. Data e ora vengono visualizzate al crawler del motore di ricerca per consentire al motore di ricerca di determinare se il record è stato aggiornato. Molti crawler utilizzano data e ora durante una ricerca per indicizzazione incrementale. Data e ora aggiornate segnala che il record è stato cambiato dopo l'ultima ricerca per indicizzazione nel record. Il crawler del motore di ricerca ignora la ricerca per indicizzazione se il record non è stato aggiornato dall'ultima ricerca per indicizzazione.

<title>

Specifica l'attributo utilizzato per il titolo della pagina dei dettagli. I motori di ricerca utilizzano questo elemento come titolo del documento che viene restituito nei risultati della ricerca. Questa voce genera un tag di <title> HTML in <head> della pagina dei dettagli. Per il documento della conoscenza, l'impostazione predefinita per il titolo è il titolo del documento della conoscenza. Il riepilogo viene utilizzato per il titolo di Incidenti, Problemi, Richieste, Ordini di cambiamento e Issue.

<meta_data>

Specifica una o più proprietà che vengono visualizzate come metadati. I metadati consentono a un motore di ricerca di archiviare caratteristiche extra del documento nel rispettivo indice. I metadati non sono oggetto di una ricerca diretta, vengono invece utilizzati per filtrare i risultati della ricerca. Questa sezione genera tag <meta> HTML in <head> della pagina dei dettagli.

Ciascuna voce nella sezione <meta_data> contiene una o più voci di <property>. Ciascun elemento di <property> è formato da un elemento <name> e un elemento <content>.

<name>

Specifica il nome della proprietà dei metadati.

<content>

Specifica l'attributo dell'oggetto che verrà utilizzato come valore per i metadati.

Insieme ciascuna coppia di elementi <name> e <content> di una <property> generano un tag <meta> HTML. I crawler del motore di ricerca utilizzano per impostazione predefinita le due proprietà dei metadati seguenti:

Descrizione

Specifica la proprietà dei metadati di un motore di ricerca che archivia un breve riepilogo del documento.

Autore

Specifica l'autore del documento.

La proprietà dei metadati CASDMTENANT viene configurata anche per impostazione predefinita per ciascun oggetto. Si tratta di una proprietà dei metadati specifica di CA SDM. Quando CA SDM viene configurato per la multi-tenancy, la superficie crawler utilizza questa proprietà per visualizzare il nome del titolare dell'oggetto al crawler del motore di ricerca. Più tardi, durante una ricerca federata, i risultati restituiti dal motore di ricerca vengono filtrati in base a questa proprietà dei metadati.

Il file XML contiene le sezioni seguenti che creano la sezione <body> di una pagina dei dettagli in CA SDM:

<additional_attributes_to_index>

Indica un elenco degli attributi dall'oggetto visualizzato dalla superficie crawler. Voci multiple separate con una virgola e uno spazio. Ad esempio, PROBLEM, RESOLUTION, SD_ASSET_ID.name.

<activity_logs>

Indica le informazioni visualizzate dalla superficie crawler dai registri attività per gli oggetti dotati di registri attività. La sezione <activity_logs> contiene gli elementi informazioni di accesso, <select_criteria>, <rel_attr> e <attributes>.

informazioni di accesso

Specifica il nome oggetto che contiene le voci del registro attività per l'oggetto. Ad esempio, l'oggetto del registro attività per:

- Incidenti, Problemi e Richieste: *alg*.
- Ordini di cambiamento: *chgalg*.
- Issue: *issalg*.
- Documenti della conoscenza: *O_COMMENTS*.

<select_criteria>

Consente di filtrare gli oggetti del registro attività visualizzati. Questo elemento è importante per aumentare la rilevanza dei risultati della ricerca diminuendo le parole che si presentano di frequente. Ad esempio, <select_criteria> per chgalg contiene la clausola Where Majic seguente:

```
"type IN ('ST', 'UPD_RISK', 'CB', 'RS', 'LOG', 'TR', 'ESC' ,'NF',
'UPD_SCHED')"
```

Questo criteri includono solo voci del registro attività che consentono a un utente di immettere commenti ed elimina le voci del registro attività con testo fisso come Iniziale o Allega documento.

<rel_attr>

Specifica la relazione di una voce del registro attività con il relativo oggetto padre. La sottosezione <rel_attr> contiene elementi di <parent_obj_attr> e <join_attr>.

<parent_obj_attr>

Indica un attributo di un registro attività che contiene un SREL (o un puntatore di chiavi esterne) all'oggetto padre. Ad esempio, change_id è l'attributo di chgalg.

<join_attr>

Indica l'attributo relazionale (Rel Attr) dell'oggetto padre archiviato in <parent_obj_attr>. Ad esempio, il <join_attr> per chgalg è l'ID. È possibile verificare questi valori mediante il comando seguente:

```
bop_sinfo -df chgalg
```

È possibile verificare entrambi i valori mediante il comando bop_sinfo -df chgalg. L'output deve mostrare che il valore per change_id è *SREL -> chg.id* e che ISS è *SREL -> iss.persistent_id.*

<attachments>

Questa sottosezione consente di visualizzare agli allegati al crawler del motore di ricerca in modo che il loro contenuto possa essere indicizzato insieme all'oggetto padre. La sezione <attachments> è consentita solo per gli oggetti che dispongono di allegati.

Gli allegati vengono gestiti in modo speciale dalla superficie crawler. Anziché inviare il contenuto di ciascun allegato al crawler dalla superficie crawler, la superficie crawler visualizza un collegamento ipertestuale che il crawler può seguire per scaricare l'allegato da CA SDM. Se durante una ricerca federata successiva un allegato viene incluso nei risultati della ricerca, facendo clic sul collegamento ipertestuale l'utente accede all'oggetto padre anziché visualizzare direttamente all'allegato.

La sezione <attachments> contiene gli elementi informazioni di accesso, <rel_attr>, <attmnt_id> e <is_parent_updated>.

informazioni di accesso

Questo elemento specifica l'oggetto Majic che collega l'allegato al rispettivo oggetto padre.

<rel_attr>

Questa sottosezione funziona come nei registri attività. Specifica il modo in cui l'oggetto padre è correlato all'oggetto che collega l'oggetto padre all'allegato.

<attmnt_id>

Questo elemento specifica l'attributo dell'oggetto di collegamento che punta all'allegato.

<is_parent_updated>

Specifica alla superficie crawler il modo in cui visualizzare la data di ultima modifica per l'oggetto. Per alcuni oggetti, come i documenti della conoscenza (Knowledge Document, KD), quando viene aggiunto un allegato, la data dell'ultima modifica del documento della conoscenza non viene aggiornata. La data dell'ultima modifica è importante quando il motore di ricerca sta eseguendo una ricerca per indicizzazione incrementale.

<configuration_items>

Viene utilizzata per gli oggetti che contengono un elenco di elementi della configurazione. Questa sezione contiene gli elementi informazioni di accesso, <rel_attr> e <attributes>.

informazioni di accesso

Funzionano come nei registri attività e negli allegati.

<rel_attr>

Funzionano come nei registri attività e negli allegati.

<attributes>

Questo elemento funziona come negli allegati.

<multi-farm_datasets>

Dopo la sezione <objects> si trova la sezione <multi-farm_datasets>. Mentre la sezione <objects> definisce gli oggetti di CA SDM e gli attributi visualizzabili con la superficie crawler, <multi-farm_datasets> specifica il modo in cui i record vengono selezionati. La sezione <multi-farm_datasets> è una raccolta di sezioni <farm>.

<farm>

Ciascuna sezione <farm> controlla le informazioni di CA SDM che vengono visualizzate a un crawler. Quando un crawler viene configurato, la sezione <farm> viene specificata nell'URL. Solo le informazioni specificate nella sezione <farm> vengono visualizzate al crawler. Ciascuna sezione <farm> contiene gli elementi <name>, <data_sets> e <sdm_user>.<name>.

Nota: Questo valore rispetta la distinzione tra maiuscole e minuscole.

<data_sets>

Specificare gli oggetti visualizzati e il modo in cui vengono selezionati i record. Questa sottosezione contiene uno o più elementi informazioni di accesso. Ciascun elemento dell'oggetto contiene un elemento <name> e <select_criteria>.

<name>

Fa riferimento a informazioni di accesso definito nella sezione <objects>.

<select_criteria>

Questo elemento specifica un criterio Majic utilizzato per selezionare i record dell'oggetto.

<sdm_user>

Questo elemento specifica l'ID utente di CA SDM da utilizzare per l'accesso alla farm. L'ID utente deve presentare il tipo di accesso crawler e un ruolo crawler.

sdm_domsrvr_name

Per un'elevata quantità di dati di indicizzazione, dedicare una gestione oggetto per la superficie crawler. Il valore predefinito è domsrvr.

sharepoint_properties_file

Questo valore corrisponde al nome del file di proprietà di SharePoint disponibile Per impostazione predefinita nella directory di CA SDM:

```
NX_ROOT\CATALINA_BASE_FS\lib
```

Contiene il parametro di configurazione utilizzato dalla ricerca federata e dalla superficie crawler in caso di configurazione multi-tenancy di CA SDM.

Nota: In caso di configurazione multi-tenancy di CA SDM, aggiornare il parametro sharepoint_version in questo file in modo che rifletta la versione di SharePoint in uso.

<list_form_number_of_records_per_object>

Utilizzare questo parametro per configurare il numero di collegamenti ipertestuali presentati dalla superficie crawler in una pagina di elenco per un oggetto.

<send_wait_timeout>

Questo valore riguarda il numero di secondi attesi dalla superficie crawler per una risposta dalla gestione oggetto prima del timeout.

Configurazione del crawler SharePoint

Configurare i crawler per effettuare una ricerca per indicizzazione e cercare il contenuto in SharePoint.

Il crawler è un'applicazione multithread con un elevato rendimento, che a volte può avere un impatto negativo sulle prestazioni di CA SDM. Per evitarlo, verificare quanto segue:

- Limitare il numero di crawler concorrenti di SharePoint che accedono alla superficie crawler in un dato momento.
- Utilizzare le regole di impatto crawler di SharePoint per limitare i crawler
- Pianificare le ricerche per indicizzazione nelle fasce orarie di minor traffico durante la giornata
- Dedicare un <sdm_domsrvr_name> di gestione oggetto alla superficie crawler nel file crawler_surface_config.xml. Per ulteriori informazioni, consultare la sezione File di configurazione XML della superficie crawler.
- Per la configurazione con disponibilità avanzata di CA SDM, dedicare un intero server applicazioni alla superficie crawler.

Procedere come descritto di seguito:

1. Creazione dell'origine di contenuto in SharePoint (a pagina 171)
2. Creazione delle regole del crawler (a pagina 172)
3. Esecuzione del crawler in SharePoint (a pagina 173)
4. Configurazione dei metadati in SharePoint (a pagina 174)
5. Verifica dei dati crawler in SharePoint (a pagina 175)

Creazione dell'origine di contenuto in SharePoint

Nota: I nomi delle impostazioni specifiche di SharePoint possono variare a seconda della versione di SharePoint in uso. Per ulteriori informazioni sulla creazione di origini di contenuto in SharePoint, consultare la documentazione di Microsoft SharePoint.

Creare origini di contenuto per identificare il tipo di contenuto elaborato dal crawler di SharePoint.

Procedere come descritto di seguito:

1. Accedere alla console di amministrazione centrale di MS SharePoint.
2. Fare clic su Gestisci applicazioni di servizio, Applicazione servizio di ricerca.
3. Fare clic su Origine contenuto per creare nuove origini di contenuto:
4. Immettere in Nome il nome di dati CA SDM per l'origine di contenuto.
5. Impostare il tipo di origine di contenuto su Siti Web.
6. Immettere l'URL seguente in Indirizzo iniziale.

   ```
   http://<sdmhostname>:<FS_TOMCAT_PORT>/fscrawl/listObject.jsp?farm=<Farm Name>
   ```

7. Per impedire al crawler di deviare dalla superficie crawler, considerare di limitare i livelli di pagina a 2 e i passaggi tra server a 1. I valori minimi consigliati per consentire la ricerca indicizzata di allegati.
8. Fare clic su Salva.

Creazione delle regole di ricerca per indicizzazione

Le regole di ricerca per indicizzazione definiscono il modo in cui si esegue la ricerca per indicizzazione dell'URL di superficie crawler Web di SharePoint. Definire le seguenti regole di ricerca per indicizzazione:

- Una regola di ricerca per indicizzazione che consente a SharePoint di effettuare una ricerca per indicizzazione sulla superficie crawler.
- Una regola di ricerca per indicizzazione che consente a SharePoint di accedere agli allegati.

Procedere come descritto di seguito:

1. Accedere alla console di amministrazione centrale di MS SharePoint.
2. Fare clic su Gestisci applicazioni di servizio, Applicazione servizio di ricerca.
3. Fare clic su Regole di ricerca per indicizzazione. Creare una nuova regola globale di ricerca per indicizzazione.
4. Immettere l'URL seguente nel browser:

   ```
   http:// <sdmhostname>:<FS_Tomcat_Port>/fscrawl/*farm=<farm-name>*
   ```

   Importante. L'URL della superficie crawler distingue tra maiuscole e minuscole. SharePoint modifica i nomi host con lettere maiuscole in minuscolo. Per SharePoint 2010, verificare che sia selezionata la casella di controllo Maiuscole/minuscole.

5. Selezionare Includi tutti gli elementi nel percorso per configurare il crawler.
6. Selezionare Esegui ricerca per indicizzazione di URL complessi, ovvero URL che contengono un punto interrogativo (?).
7. Selezionare Specifica un account di accesso contenuto diverso.
8. Immettere il nome dell'account utente di CA SDM e la password per la superficie crawler.
9. Creare una seconda regola di ricerca per indicizzazione per gli allegati di CA SDM:

   ```
   http://<sdmhostname>:<FS_TOMCAT_PORT>/CAisd/*
   ```

10. Specificare l'autenticazione predefinita:

    Nota: La superficie crawler utilizza l'autenticazione di base. Il daemon del repository di CA SDM utilizza protezione BOPSID proprietaria non supportata direttamente da SharePoint. Specificare un ID utente e una password o scegliere l'accesso anonimo se disponibile nella versione di SharePoint in uso.

    - Per SharePoint 2013, selezionare Specifica un account di accesso contenuto diverso. Selezionare l'opzione Accesso anonimo.
    - Per SharePoint 2010, utilizzare l'account di accesso al contenuto predefinito (NT AUTHORITY\NETWORK SERVICE).

    La regola di ricerca per indicizzazione di Microsoft SharePoint è stata creata.

Avvio di ricerca per indicizzazione in SharePoint

Avviare una ricerca per indicizzazione completa o incrementale delle origini di contenuto in SharePoint per indicizzare il contenuto di ricerca.

Procedere come descritto di seguito:

1. Accedere alla pagina di amministrazione centrale di SharePoint.
2. Fare clic su Gestisci applicazioni di servizio, Applicazione servizio di ricerca.
3. Fare clic su Origini contenuto. Selezionare l'origine di contenuto configurata per la superficie crawler di SharePoint.
4. Selezionare **Avvia ricerca per indicizzazione completa** o **Avvia ricerca per indicizzazione incrementale**.

   Una ricerca per indicizzazione completa viene eseguita sul contenuto intero compreso in un'origine di contenuto. Le ricerche per indicizzazione complete richiedono più tempo e risorse per il completamento rispetto alle ricerche per indicizzazione incrementali.

   In una ricerca per indicizzazione incrementale, l'indice rimane intatto e il crawler esegue la ricerca solo sul contenuto aggiunto o modificato dall'ultima ricerca per indicizzazione eseguita correttamente. Per ulteriori informazioni, consultare la documentazione di Microsoft SharePoint.

Configurazione dei metadati in SharePoint

Nota: Questo argomento riguarda solo gli ambienti multi-tenancy di CA SDM.

Quando il crawler rileva metadati di CA SDM, questi vengono archiviati in SharePoint come Proprietà sottoposte a ricerca per indicizzazione. Queste proprietà vengono rilevate durante l'iniziale ricerca per indicizzazione completa della superficie crawler di CA SDM. Il crawler di SharePoint rileva i metadati e crea le proprietà ricercate per indicizzazione.

I metadati vengono utilizzati per trasmettere informazioni aggiuntive al crawler nelle pagine dei dettagli mediante il tag <meta> nella sezione <head>. Queste informazioni sono disponibili per la ricerca e il filtraggio. Se CA SDM è configurato per la multi-tenancy, la superficie crawler visualizza solo le informazioni sui metadati del titolare.

Quando si esegue una ricerca federata, il nome del titolare viene inviato al motore di ricerca per filtrare i risultati in modo corretto.

Procedere come descritto di seguito:

1. Accedere alla console di amministrazione centrale di MS SharePoint.
2. Fare clic su Gestisci applicazioni di servizio, Applicazione servizio di ricerca, Metadati (SharePoint 2010) o Schema di ricerca (SharePoint 2013).
3. Verificare che la ricerca per indicizzazione di SharePoint sia stata eseguita correttamente per i dati di CA SDM.
4. Fare clic su Proprietà gestite.
5. Fare clic su Nuova proprietà gestita.
6. Immettere CASDMTENANT come Nome proprietà.

   CASDMTENANT indica il nome del titolare per l'oggetto di CA SDM. Le informazioni sul titolare secondario non vengono visualizzate.
7. Selezionare Testo come Tipo proprietà.
8. Scorrere giù. Fare clic su Aggiungi mapping.
9. Cercare la proprietà di ricerca per indicizzazione CASDMTENANT e selezionarla.
10. Fare clic su OK per salvare la nuova proprietà gestita.

    I metadati in SharePoint sono configurati.

Verifica dei dati crawler in SharePoint

Verificare i dati crawler in SharePoint per visualizzare i risultati di ricerca.

Procedere come descritto di seguito:

1. Accedere come amministratore Service Desk di CA SDM.
2. Fare clic sulla scheda Gestione della conoscenza per un ticket nuovo o esistente.
3. Selezionare l'origine di ricerca SharePoint.
4. Immettere la chiave di ricerca. Fare clic su Cerca.

   Il crawler visualizza i risultati di ricerca.

Risoluzione dei problemi

La superficie crawler presenta la solita matrice dei file di registro:

1. Se si desidera abilitare il debug per la ricerca confederata, accedere alla seguente directory di <USDK:

   ```
   $NX_ROOT\bopcfg\www\CATALINA_BASE_FS\webapps\cafedsearch\WEB-INF
   ```

2. Aprire il file log4j.properties e modificare le informazioni relative alla modalità di debug.
3. Per abilitare il debug per fscrawl, accedere alla seguente directory di CA SDM:

   ```
   $NX_ROOT\bopcfg\www\CATALINA_BASE_FS\webapps\fscrawl\WEB-INF
   ```

4. Aprire il file log4j.properties e modificare le informazioni relative alla modalità di debug.
5. Per correggere gli errori di sintassi riscontrati durante la configurazione della superficie crawler di SharePoint, aprire il file di registro jfscrawl dalla directory di CA SDM:

   ```
   $NX_ROOT\logs directory
   ```

6. Se si individuano errori di sintassi, correggere il file XML e riavviare il server Tomcat di ricerca federata. Il registro si trova in

   ```
   $NX_ROOT\logs\jfscrawl.log
   ```

   Ad esempio, se un tag di <meta_data> viene danneggiato accidentalmente, il registro riporta l'errore seguente:

   ```
   08/06 15:43:52,624 [pool-2-thread-1] ERROR FSCrawlApplicationListener 302
   XmlException::Problem loading
   config_file::C:\PROGRA~2\CA\SERVIC~1\bopcfg\www\CATALINA_BASE_FS\webapps\fscr
   awl\WEB-INF\crawler_surface_config.xml:274:8: error: </meta_dataxxxxx> does not
   close tag <meta_data>
   ```

   ```
   08/06 15:43:52.625 [pool-2-thread-1] ERROR FSCrawlApplicationListener 144
   crawler_surface_config.xml could not be loaded, cannot read.
   ```

7. In assenza di errori di sintassi, viene visualizzato il messaggio seguente:

   ```
   08/06 15:46:27.924 [pool-2-thread-1] INFO FSCrawlApplicationListener 58 fscrawl
   context had been loaded successfully.
   ```

8. Correggere eventuali altri errori non visibili fino a quando si tenta di accedere a CA SDM.

   Ad esempio, è stata richiesta la visualizzazione di un attributo xxxxx sconosciuto per gli Incidenti nell'elemento <additional_attributes_to_index> del file crawler_surface_config.xml. L'applicazione di superficie crawler non rileva l'errore. Ma quando la superficie crawler invia la richiesta alla gestione oggetto, l'errore viene rilevato e riportato nel file stdlog.x come indicato di seguito:

```
08/06 15:51:23.92 SDMSERVER domsrvr 10860 ERROR domset.c 8049 Unknown attribute
"xxxxx" requested from domset MLIST_STATIC of factory
```

9. Utilizzare il comando bop_sinfo -d per risolvere l'errore.
10. Modificare il file crawler_surface_config.xml.
11. Riavviare il server Tomcat della ricerca federata.

    Gli oggetti della superficie crawler vengono configurati correttamente.

Creazione di un nuovo adapter personalizzato mediante l'interfaccia SDK

Importante. Il codice sorgente di esempio per il Software Development Kit di ricerca federata di CA viene fornito ai clienti per la creazione e la distribuzione di adapter personalizzati alternativi. Tuttavia, il supporto tecnico di CA non fornirà assistenza per la scrittura del codice personalizzato effettivo. La creazione e la distribuzione di adapter aggiuntivi non è supportata attivamente. Vengono forniti unicamente i codici sorgente di esempio SDK inclusi con l'applicazione CA Service Desk Manager.

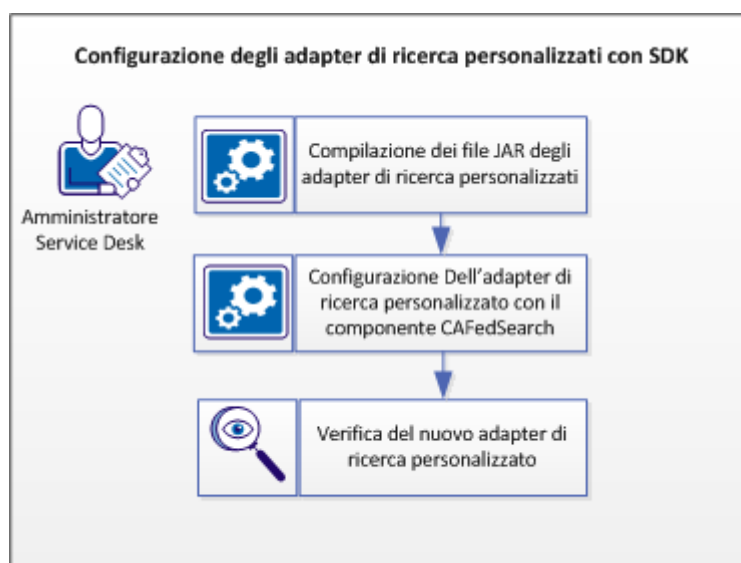
L'architettura SDK per la ricerca federata di CA è progettata ai fini dell'estensibilità. SDK contiene tutti i file JAR necessari per sviluppare un adapter personalizzato. È possibile importare i progetti Eclipse di esempio e, inoltre, sono disponibili le destinazioni di build Ant per generare adapter di ricerca personalizzati. Il SDK si trova nella directory di CA SDM:

```
$NX_ROOT\samples\sdk\fedsearch\adapters-source.tar.gz
```

È possibile utilizzare il codice sorgente dei seguenti adapter per la scrittura di nuovi adapter personalizzati:

- Google
- CA Open Space
- Microsoft SharePoint

Nota: Il codice sorgente per il servlet CAFedSearch, il framework sottostante e il filtro di protezione non vengono forniti. Non viene fornito alcun codice sorgente per i componenti di superficie crawler.

Il componente SDK è scritto in Java e condiviso come file JAR (cafedsearch-adapter-sdk-1.0.0.jar). Il SDK offre un'interfaccia semplice che consente ai clienti di sviluppare e distribuire i propri adapter di ricerca.

Procedere come descritto di seguito:

1. Compilazione dei file JAR per l'adapter di ricerca personalizzato (a pagina 180)
2. Configurazione del nuovo adapter di ricerca personalizzato con il componente CAFedSearch (a pagina 183)
3. Verifica del nuovo adapter di ricerca personalizzato (a pagina 185)

Compilazione dei file JAR per il nuovo adapter personalizzato

Compilare i file JAR del nuovo adapter personalizzato.

Procedere come descritto di seguito:

1. Compilare il nuovo adapter di ricerca personalizzato. Verificare i seguenti file JAR siano disponibili nel Classpath di Java:

   jsr311-api-1.0.jar

   Questo file JAR è disponibile nella directory di CA SDM:

   `%NX_ROOT%\java\lib\CXF\`

   cafedsearch-core.jar

   Questo file è disponibile nella directory:

   `%NX_ROOT%\bopcfg\www\CATALINA_BASE_FS\webapps\cafedsearch\WEB-INF\lib`

   cafedsearch-adapter-sdk-1.0.0.jar

   Questo file è disponibile nella directory:

   `%NX_ROOT%\bopcfg\www\CATALINA_BASE_FS\webapps\cafedsearch\WEB-INF\lib`

   log4j-1.2.15.jar (facoltativo)

   Questo file è disponibile nella directory:

   `%NX_ROOT%\java\lib`

2. Eseguire la scrittura di una nuova classe Java per estendere la classe SearchAdapter e fornire l'implementazione del metodo astratto.

   `search`

   Il componente CAFedSearch richiama e trasmette i parametri del metodo di ricerca. Questi parametri sono integrati all'interno del parametro SearchOptions per ciascuna richiesta di ricerca dal client.

   Nota: Verificare che l'implementazione sia thread-safe in quanto il componente CAFedSearch è in grado di gestire unicamente un'istanza della classe Java. Per ciascuna operazione di ricerca, il metodo di ricerca viene richiamato sulla stessa istanza.

3. Il parametro SearchOptions per il metodo di ricerca comprende i metodi seguenti:

   getSearchTerms()

   Specifica il metodo per il recupero della stringa di ricerca.

   getStartIndex()

   Specifica il metodo di indicizzazione iniziale, il numero in base al quale il client desidera cercare gli elementi. L'indice inizia da 1.

   getItemsPerPage()

   Specifica il numero massimo di risultati della ricerca previsti dal client.

Nota: È possibile utilizzare anche altri metodi di classe Java. Ad esempio: getUserId()

4. Inviare le informazioni raccolte all'API del motore di ricerca esterno per recuperare i risultati della ricerca.

   Nota: Per informazioni sui metodi di classe Java, consultare la documentazione di Java.

5. Il metodo di ricerca restituisce un'istanza della classe ResultCollection. Creare un'istanza di ResultCollection e inserire i valori mediante i metodi seguenti:

   setSources(String name)

   Specifica il nome dell'adapter di ricerca. I nomi rispettano la distinzione tra maiuscole e minuscole e devono corrispondere esattamente al nome specificato nel file di configurazione dell'utilità. Per comodità, SearchAdapter fornisce un metodo getName() da utilizzare.

   Ad esempio:

   ```
   results.setSources(getName());
   ```

   setTotalResults (int total)

   Specifica il numero totale dei risultati di ricerca.

   setStartIndex(int startIndex)

   Specifica un indice iniziale dei risultati. Questo valore si basa sui risultati forniti dal motore di ricerca.

   ```
   results.setStartIndex(startIndex);
   ```

6. È necessario trasmettere la raccolta di ResultItems all'oggetto ResultCollection chiamando il metodo setSearchResultItems. Per aggiungere un'istanza di ResultItem alla volta, utilizzare il metodo addSearchResultItem().

   Nota: Per ulteriori informazioni sulla classe Java di ResultCollection, consultare la documentazione di Java.

7. La classe ResultItem presenta i seguenti metodi importanti, che vanno riempiti per ciascun elemento dei risultati della ricerca (riga).

   setContentText(String txt)

   Specifica un metodo per impostare il contenuto effettivo dei risultati di ricerca.

   setContentHTML(String txt)

   Specifica un metodo per impostare il contenuto HTML (può contenere i tag HTML). Se il motore di ricerca restituisce l'HTML evidenziato, impostare il testo evidenziato mediante questo metodo.

   Nota: Se il motore di ricerca non dispone di questa funzionalità, è possibile scrivere un metodo semplice di classe Java per evidenziare il testo. L'adapter CA Open Space dispone di un metodo semplice con termini in grassetto nei risultati di ricerca.

setTitleHTML(String titleHTML)

Metodo per impostare un titolo HTML (può contenere tag HTML).

setTitleText(String titleText)

Metodo per impostare un titolo normale (non può contenere tag HTML).

setSource(String source)

Metodo per impostare l'attributo di origine. Un'attivazione tipica sarebbe setSource(getName()); per un elemento

Nota: Se l'adapter di ricerca richiede più file JAR, personalizzare il file build.xml per compilare e preparare un file JAR per l'adapter. È necessario disporre di Ant binari per utilizzare il file build.xml. Usare Ant per eseguire le destinazioni nel file build.xml per compilare e creare i file JAR. Conservare il file build.xml insieme alla cartella di origine (src). Il file build.properties è facoltativo. Per ulteriori informazioni su binari Ant, consultare la Guida in linea di Ant.

Il file JAR è stato correttamente compilato.

Configurazione del nuovo adapter di ricerca personalizzato con il componente CAFedSearch

Configurare il file JAR per il nuovo adapter di ricerca personalizzata con il componente CAFedSearch per creare le origini di ricerca di CA SDM.

Procedere come descritto di seguito:

1. Copiare il file JAR dalla posizione dist\lib (creato nella fase di compilazione dei file JAR del nuovo adapter di ricerca personalizzata) nella seguente directory di CA SDM:

   `%NX_ROOT%\bopcfg\www\CATALINA_BASE_FS\webapps\cafedsearch\WEB-INF\lib`

2. Accedere alla seguente directory di CA SDM:
   `$NX_ROOT\sample\cafedsearch\`

3. Creare un nuovo file modello XML per l'adapter di ricerca personalizzata. Ad esempio, il file XYZ-tmpl.xml.

4. Il file modello predefinito contiene quanto segue:

```
<?xml version="1.0" encoding="UTF-8"?>

<beans default-autowire="byName"
xsi:schemaLocation="http://www.springframework.org/schema/beans

http://www.springframework.org/schema/beans/spring-beans-2.5.xsd

http://cxf.apache.org/core

http://cxf.apache.org/schemas/core.xsd

http://cxf.apache.org/jaxrs

http://cxf.apache.org/schemas/jaxrs.xsd"
xmlns:cxf="http://cxf.apache.org/core"

xmlns:jaxrs="http://cxf.apache.org/jaxrs"

xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

xmlns="http://www.springframework.org/schema/beans">


    <bean autowire="autodetect"

            class=" com.abc.xyz.XYZAdapter "

                    id="XYZAdapterConfiguration" scope="singleton">

<property name="username" value="$(xyz_username)"/>

    <property name="password" value="$(xyz_password)"/>

</bean>

<bean autowire="autodetect" class="com.abc.xyz.XYZAdapter"
id="XYZSearchAdapter" init-method="init" destroy-method="destroy"
depends-on="XYZAdapterConfiguration">
```

```
                    <property name="config"
ref="OpenSpaceAdapterConfiguration" />
    </bean>
</beans>
```

5. È possibile creare valori di proprietà basati sui valori di input forniti per gli adapter di ricerca nella fase 4.

   Aggiungere xyz_username e xyz_password nel file adapters.properties e specificare i valori per la proprietà.

6. Eseguire il file dell'utilità per generare la configurazione XML per gli adapter di ricerca personalizzata:

   ```
   fs_adapters_cli -i -k XYZ –b XYZSearchAdapter -t "XYZ-tmpl.xml " -o "xyz.xml
   ```

7. Il file xyz.xml viene creato e registrato nel file adapters-config.xml.

8. Copiare i file xyz.xml e adapters-config.xml nella seguente directory di CA SDM: `$NX_ROOT\samples\cafedsearch\WEB-INF`

9. Immettere il comando seguente per riavviare i servizi di Tomcat federati:
   ```
   pdm_tomcat_nxd –c STOP –t FS
   pdm_tomcat_nxd –c START –t FS
   ```

10. Creare le origini di ricerca federata per l'adapter XYZ nell'interfaccia utente di CA SDM.

    Per ulteriori informazioni sulle origini di ricerca federata, consultare la sezione Creazione delle origini di ricerca federata in CA SDM (a pagina 157).

11. In CA SDM, accedere alla scheda Gestione della conoscenza. Selezionare la casella di controllo XYZ ed eseguire le operazioni di ricerca.

    Il nuovo adapter di ricerca personalizzata è stato configurato correttamente con il componente CAFedSearch.

Verifica del nuovo adapter di ricerca personalizzato

Verificare la funzionalità del nuovo adapter di ricerca personalizzato mediante il client REST.

Procedere come descritto di seguito:

1. Scaricare il client REST da Internet:

   https://code.google.com/p/rest-client/

2. Avviarlo mediante Java (è richiesto JRE).
3. Immettere l'URL seguente nell'interfaccia utente di client REST:

   ```
   http://sdmhostname:<FS_Tomcat_Port>/cafedsearch/sdm/search?q=search&userid=<sdmuserid>&source=<Adapter Name>
   ```

4. Spegnere l'interruttore di protezione di CA SDM. Aprire il file seguente per la modifica e l'inserimento di commenti nella sezione <jaxrs:inInterceptors>:

   ```
   $NX_ROOT\bopcfg\www\CATALINA_BASE_FS\webapps\cafedsearch\WEB-INF\beans.xml
   ```

   Nota: La disattivazione del filtro di protezione in un ambiente di produzione non è consigliata. Disattivare il filtro di protezione in un ambiente di test per verificare la funzionalità del nuovo adapter di ricerca personalizzato.

5. Verificare che il nuovo adapter di ricerca personalizzato funzioni correttamente. Se i risultati di ricerca non vengono visualizzati, consultare i registri oppure impostare il livello di registro su Debug.

Aggiunta di un filtro CORS

La funzionalità Ricerca federata viene configurata nell'interfaccia del client Web con l'aggiunta del filtro Cross-Origin Resource Sharing (CORS)all'interfaccia Web e al server Tomcat di ricerca federata (Federated Search, FS). Questo filtro consente di aggiungere un elenco di richieste multiorigine. Per impostazione predefinita, l'interfaccia Web consente le richieste multiorigine o ad origine unica. Tale impostazione è indicata mediante un simbolo di asterisco (*). Si consiglia di limitare questa impostazione specificando un elenco di server dell'interfaccia Web CA SDM configurati per l'ambiente in uso.

Per modificare l'impostazione del client di interfaccia Web e consentire le richieste multiorigine, completare le operazioni riportate di seguito.

Procedere come descritto di seguito::

1. Accedere alla seguente directory di CA SDM per modificare le impostazioni dell'interfaccia Web:

   ```
   $NX_ROOT\bopcfg\www\CATALINA_BASE_FS\webapps\cafedsearch\WEB-INF\web.xml
   ```

2. Aprire il file web.xml e cercare il seguente elemento:

   ```
   <web-app><filter><init-param><param-name>cors.allowOrigin</param-name>
   ```

3. Aggiornare il tag <param-value> con un elenco di domini separati da spazio. Esempio di indirizzo URL di base per l'interfaccia Web:

   ```
   <param-value>http://web01:8080 http://web02:8080
   http://web03:8080</param-value>
   ```

4. Salvare il file web.xml. Tomcat viene riavviato automaticamente.
5. Testare e verificare la configurazione della ricerca federata sull'interfaccia del client Web. Verificare il corretto funzionamento.
6. Per conservare gli aggiornamenti dell'interfaccia Web in seguito all'esecuzione della configurazione di CA SDM, applicare gli stessi aggiornamenti al file web.xml.tpl.

Chiamata del servlet CAFedSearch tramite REST

Il servlet CAFedSearch presenta un'interfaccia RESTful che consente di inviare le richieste di ricerca tramite client di ricerca personalizzati, programmi e interfacce utente.

Questa interfaccia RESTful accetta solo le richieste HTTP Collection GET che seguono la specifica di OpenSearch. Sono supportate le risposte JSON e XML. Ogni richiesta deve contenere un token BOPSID di Service Desk che è possibile ottenere dai servizi Web SOAP o RESTful di CA SDM.

Procedere come descritto di seguito:

1. Acquisire un token BOPSID mediante servizi Web RESTful di CA SDM.
2. Acquisire una chiave di accesso REST inviando una richiesta HTTP POST sulla risorsa rest_access con le credenziali di accesso.

   Inoltre, è possibile ottenere un token BOPSID con la chiave di accesso REST inviando una richiesta HTTP POST sulla risorsa bopsid.
3. Per informazioni sull'invio delle richieste ai servizi Web RESTful di CA SDM, consultare i file di esempio nella seguente directory di CA SDM:

   ```
   NX_ROOT\samples\sdk\rest\java
   ```
4. Per utilizzare l'API di ricerca federata per eseguire una ricerca, inviare una richiesta HTTP GET sulla risorsa di ricerca, trasferire i criteri di ricerca e il token BOPSID tramite l'URL di CA SDM.
   GET

   ```
   http://<sdmhostname>:<FS_TOMCAT_PORT>/cafedsearch/sdm/search?q=<searchTerms>&
   source=<adapterName>&BOPSID=<bopsidToken>&userid=<userId>
   ```

   searchTerms

   Specifica un elenco di parole chiave delimitato da spazi. Deve essere codificato con URL.

   adapterName

   Specifica il nome del motore di ricerca indicato nel campo Codice origine di ricerca del record mediante l'utilità di configurazione degli adapter.

   Altri argomenti supportati sono i seguenti:

   index

   Specifica il primo indice desiderato nei risultati di ricerca. Deve essere un numero intero maggiore o uguale a 1.

   page

   Specifica la prima pagina desiderata nei risultati di ricerca. Deve essere un numero intero maggiore o uguale a 1.

size

Specifica il numero di risultati per pagina desiderati dal client di ricerca.

type

I valori validi: JSON o XML.

Capitolo 7: Implementazione delle policy

Questa sezione contiene i seguenti argomenti:

Implementazione dei criteri (a pagina 189)

Implementazione dei criteri

Un elemento principale della configurazione del service desk consiste nell'implementazione dei criteri nel rispetto delle esigenze del processo aziendale corrente.

CA SDM fornisce un'implementazione predefinita dei criteri adatta ad alcuni siti e funge da valido punto di partenza per altri. Esaminare l'implementazione predefinita in tutte le aree di definizione dei criteri per identificare le parti che potrebbero soddisfare le esigenze e le parti da modificare.

Notifiche

Con CA Service Desk Manager è possibile inviare al personale appropriato notifiche sulle attività dei ticket (attività di ricerca, escalation e così via) e sugli eventi dei ticket (ad esempio l'apertura di un ticket). È anche possibile inviare al personale appropriato notifiche sulla scheda Report della conoscenza e sulle sessioni di assistenza di Support Automation. Quando viene eseguita un'attività o si verifica un evento significativo, CA Service Desk Manager crea un messaggio di notifica che:

- Identifica l'attività del ticket o l'evento di notifica
- Fa riferimento al ticket
- Include altre informazioni facoltative
- Identifica potenziali contatti.

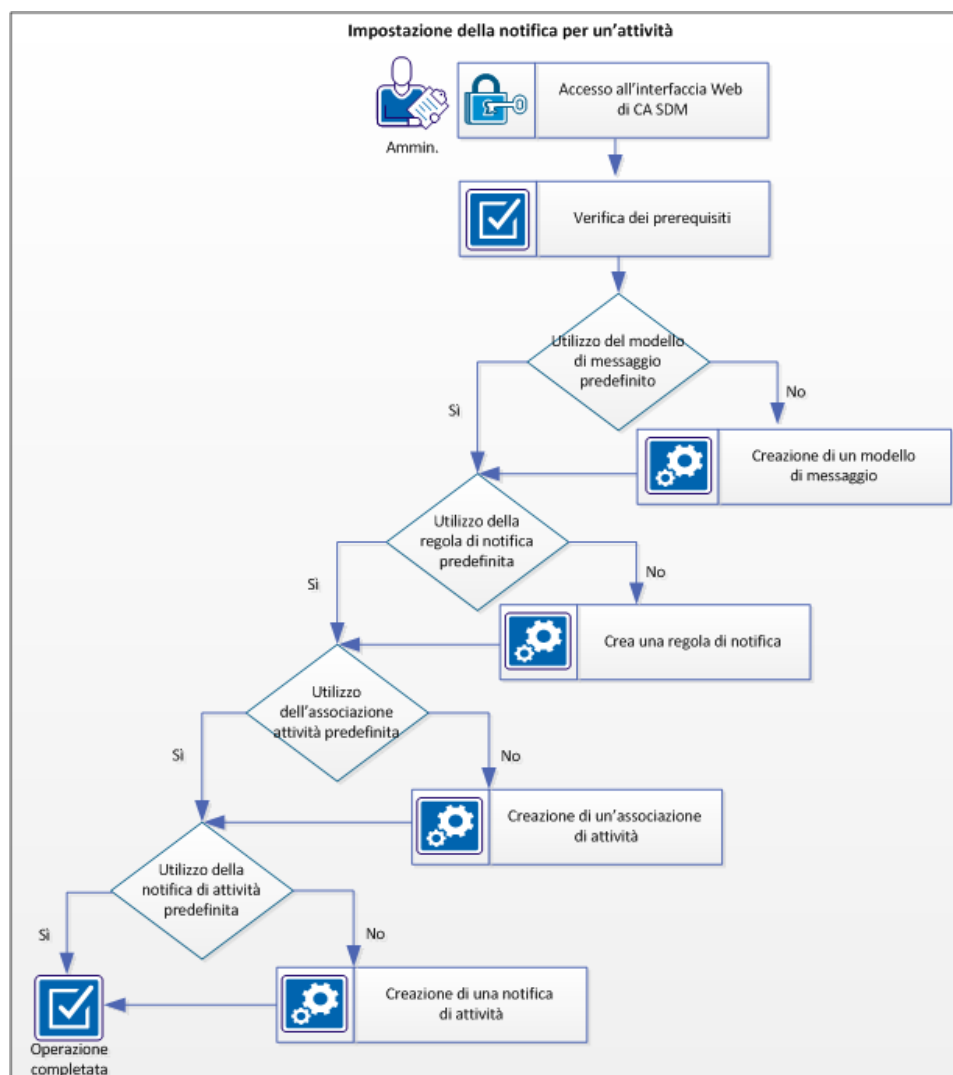
È possibile visualizzare un messaggio di notifica relativa ad un'azione di sistema per un ticket. Per azioni di sistema si intendono l'apertura, la chiusura e la modifica di un ticket tramite le relative informazioni cronologiche.

L'impostazione delle notifiche automatiche implica le seguenti attività:

- Definizione delle notifiche attività che determinano i tipi di attività che generano le notifiche.
- Definizione delle notifiche contatto oggetto che determinano i contatti oggetto che possono essere utilizzati per inviare notifiche in una notifica attività.
- Identificazione dei metodi utilizzati per l'invio dei messaggi.

Configurazione di una notifica per un'attività

È possibile definire una notifica inviata per una specifica attività. Un'attività è un'azione eseguita da una persona, come la soluzione di un ticket, l'invio di un'indagine gestita, l'esecuzione della scheda Report della conoscenza e così via. Le attività quotidiane, ad esempio la risposta a una chiamata, l'annullamento e la chiusura di un record, l'aumento della priorità o l'aggiornamento dello stato possono provocare l'invio di una notifica.

Il diagramma seguente mostra come configurare una notifica per un'attività:

Procedere come descritto di seguito:

1. Aprire l'interfaccia utente Web di CA SDM (a pagina 191).
2. Verificare i prerequisiti (a pagina 191).
3. Se non si desidera utilizzare un modello di messaggio predefinito, creare un modello di messaggio (a pagina 194).
4. Se non si desidera utilizzare una regola di notifica predefinita, creare una regola di notifica (a pagina 196).
5. Se non si desidera utilizzare un'associazione di attività predefinita, creare un'associazione attività (a pagina 198).
6. Se non si desidera utilizzare una notifica di attività predefinita, creare una notifica di attività (a pagina 198).

Apertura dell'interfaccia utente Web di CA SDM

Accedere all'interfaccia utente Web dai server seguenti, in base alla configurazione di CA SDM:

- Convenzionale: server primario o secondario
- Disponibilità avanzata: server applicazioni o in background

Verifica dei prerequisiti

Verificare i prerequisiti seguenti prima di iniziare la configurazione:

- L'opzione di aggiunta URL nella notifica è stata installata (a pagina 191).
- Il metodo di notifica per il destinatario è stato verificato (a pagina 192).
- Se si desidera inviare una notifica manuale a un indirizzo di posta elettronica che non è associato a un contatto, consentire gli indirizzi di posta elettronica temporanei (a pagina 192)

Installazione dell'opzione di aggiunta URL nella notifica

Il campo web_url presente nelle tabelle Change_Request e Workflow_Task contengono un valore URL che consente all'utente di accedere a un determinato ordine di cambiamento o attività del flusso di lavoro tramite l'interfaccia Web. Quando gli URL vengono utilizzati nelle notifiche di posta elettronica, l'utente può fare clic sull'URL per accedere all'interfaccia Web senza ulteriori query.

Prima di poter implementare i collegamenti ipertestuali URL nelle notifiche, configurare il sistema nel modo seguente:

1. Installare e configurare l'interfaccia Web CA SDM. Per ulteriori informazioni sulla configurazione dell'interfaccia Web di CA SDM, consultare la *Guida all'implementazione*.
2. Utilizzando Gestore opzioni, configurare e installare l'opzione web_cgi_url per specificare l'ubicazione del motore Web CA SDM. Ad esempio, http://hostname/scripts/pdmcgi.exe. Per la configurazione di disponibilità avanzata, il nome host dovrebbe indicare il server applicazioni o l'utilità di bilanciamento del carico.

Verifica del metodo di notifica per il destinatario

Assicurarsi che il contatto a cui si desidera inviare la notifica sia assegnato a quel particolare metodo di notifica.

Procedere come descritto di seguito:

1. Selezionare Gestione protezione e ruoli, Contatti nella scheda Amministrazione.

   Viene visualizzata la pagina Ricerca contatto.
2. Cercare il contatto utilizzando il filtro e, tra i risultati della ricerca, selezionare il contatto a cui si desidera inviare la notifica.

   Viene visualizzata la pagina dei dettagli del contatto.
3. Selezionare Notifica nella scheda Dettagli di contatto.
4. Verificare il metodo di notifica. In base alla priorità di notifica, scegliere l'opzione richiesta. Ad esempio, si desidera inviare una notifica di posta elettronica per ogni notifica di emergenza. Selezionare l'opzione Posta Elettronica nel campo Emergenza.
5. Per modificare il metodo di notifica, fare clic su Modifica, modificare l'opzione, quindi fare clic su Salva.

   Il metodo di notifica per il contatto viene verificato.

Consenso a indirizzi di posta elettronica temporanei

Un indirizzo di posta elettronica temporaneo è un indirizzo non associato a un contatto nel sistema. Gli indirizzi di posta elettronica temporanei sono utili in circostanze come quelle riportate di seguito:

- Un utente finale è fuori ufficio oppure ha difficoltà ad accedere al proprio account di posta elettronica standard.
- L'analista vuole utilizzare la posta elettronica per tenere traccia delle interazioni con l'utente.

- L'analista invia una notifica manuale a un indirizzo di posta elettronica *temporaneo* dell'utente.
- L'analista può visualizzare il registro delle attività, che viene aggiornato con la notifica manuale.

I destinatari non possono rispondere a indirizzi temporanei quando il rispettivo indirizzo di posta elettronica non è associato al record di un contatto o non dispongono delle autorizzazione necessarie per modificare il ticket.

Nota: gli indirizzi di posta elettronica temporanei sono sempre indirizzi di posta elettronica SMTP e sono supportati solo quando il Metodo preferito supporta SMTP. Per ulteriori informazioni sulla modalità di configurazione degli indirizzi di posta elettronica temporanei, consultare la *Guida in linea*.

Procedere come descritto di seguito:

1. Selezionare Gestione opzioni, Notifiche, nella scheda Amministrazione.

   Viene visualizzata la pagina Elenco Opzioni.

2. Fare clic su notification_allow_temp_address.

   Viene visualizzata la pagina Dettagli opzioni notification_allow_temp_address.

3. Fare clic su Modifica.
4. Fare clic su Installa.

   Viene visualizzata la pagina Dettagli opzioni notification_allow_temp_address.

5. Fare clic su Chiudi finestra.
6. Riavviare i server di CA SDM. Per ulteriori informazioni su come avviare il server di CA SDM, a seconda della configurazione di CA SDM, consultare lo scenario *Riavvio dei server di CA SDM* o consultare le informazioni nella *Guida per l'amministratore*.

   È ora consentito utilizzare indirizzi di posta elettronica temporanei per le notifiche manuali.

Creazione di un modello di messaggio

Creare un modello di messaggio che contenga i valori da utilizzare per il messaggio di notifica. Quando si inviano più messaggi di notifica, è possibile usare i modelli messaggio per semplificare il carico di lavoro.

Nota: in caso di installazione dell'opzione multi-tenancy, selezionare il titolare appropriato dall'elenco a discesa. L'opzione pubblica (condivisa) consente di creare l'oggetto per tutti i titolari.

Procedere come descritto di seguito:

1. Selezionare Notifiche, Modelli messaggio dalla scheda Amministrazione.

   Viene visualizzata la pagina Elenco Modelli messaggio.

2. Fare clic su Crea Nuovo.

   Viene visualizzata la pagina Crea Nuovo modello di messaggio.

3. Compilare i campi in modo appropriato.

   Simbolo

   Definisce un identificatore univoco per questo modello di messaggio.

   Tipo di oggetto

   Specifica il tipo di oggetto associato a questo modello. Ad esempio, selezionare Richiesta/ Incidente/ Problema per qualsiasi notifica collegata a un ticket.

   Stato record

   Specifica se lo stato del modello è attivo o inattivo. Impostare lo stato su Attivo per utilizzare il modello di messaggio.

   Notifica automatica

   Specifica di inviare la notifica associata al modello automaticamente, quando l'attività viene eseguita. Ad esempio, l'utente ha impostato una notifica iniziale, l'oggetto da notificare e il modello del messaggio, ma non desidera ancora attivare le notifiche. In questo caso l'utente non seleziona Notifica automatica. Quando l'utente desidera avviare le notifiche automatiche, seleziona la casella di controllo corrispondente. La notifica viene attivata ed eseguita come definito.

   Livello notifica

   Specifica l'importanza relativa dell'invio di questa notifica. Ad esempio, selezionare Emergenza se si desidera inviare la notifica di posta elettronica al contatto non appena l'attività associata si verifica.

   Titolo messaggio di notifica

   Specifica il titolo del messaggio. È possibile utilizzare variabili per inserire il numero dell'incidente nel titolo del messaggio. Ad esempio, @{call_req_id.type.sym} @{call_req_id.ref_num} @{type.sym}.

Testo del messaggio di notifica

Specifica il contenuto del messaggio. È possibile utilizzare variabili per inserire il nome dell'analista, il nome dell'utente finale e la descrizione nel messaggio. Ad esempio:

```
@{call_req_id.type.sym} @{call_req_id.ref_num} @{type.sym}.

Assegnato a: @{call_req_id.assignee.combo_name}

Cliente: @{call_req_id.customer.combo_name}

Descrizione: @{call_req_id.description}


Fare clic sull'URL seguente per visualizzare:

@{call_req_id.web_url}
```

È possibile utilizzare la parola chiave ARTIFACT per specificare come vengono gestiti gli elementi nei messaggi in uscita, nei modelli di messaggio, nelle notifiche e nelle risposte automatiche. La parola chiave ARTIFACT utilizza i seguenti valori:

- **NONE**—Specifica nessuna convalida degli elementi. Questo valore equivale a non utilizzare alcun valore.
- **PROTECTED**—Convalida un ticket nei confronti dell'hash per conferma. Se la conferma non riesce, l'elemento è considerato non valido e il filtro non riesce quando si filtra alla ricerca di un elemento ({{object_id}}).
- **SECURE**—Esegue la decrittografia del numero ticket. Se il valore non è una password valida, l'elemento è considerato non valido e il filtro non riesce quando si filtra alla ricerca di un elemento ({{object_id}}).

Messaggio HTML

Specifica il messaggio HTML che vedrà il destinatario. Se il destinatario riceve il messaggio su un dispositivo esterno, come un telefono cellulare o PDA, il messaggio viene visualizzato soltanto in formato di testo semplice. Fare clic su Edit HTML Message (Modifica messaggio HTML) per aprire l'Editor HTML.

Visualizzazione rapida

Mostra il messaggio così come viene visualizzato dal destinatario.

Origine HTML

Mostra il messaggio nel codice di origine HTML.

4. Fare clic su Salva.

Il modello del messaggio viene creato.

Creazione di una regola di notifica

Creare la regola di notifica per specificare i contatti a cui inviare la notifica e in quali circostanze.

Nota: in caso di installazione dell'opzione multi-tenancy, selezionare il titolare appropriato dall'elenco a discesa. L'opzione pubblica (condivisa) consente di creare l'oggetto per tutti i titolari.

Procedere come descritto di seguito:

1. Selezionare Notifiche, Regole di notifica dalla scheda Amministrazione.

   Viene visualizzata la pagina Elenco Regole di notifica.

2. Fare clic su Crea Nuovo.

   Viene visualizzata la pagina Crea Nuova regola di notifica.

3. Inserire i dati nei seguenti campi:

   Simbolo

   Definisce un identificatore univoco per la regola di notifica. Ad esempio, immettere Aggiornamento descrizione ticket.

   Tipo di oggetto

   Definisce l'oggetto al quale si applica la regola. Ad esempio, selezionare Richiesta/ Incidente/ Problema per un'attività collegata a un ticket.

4. Fare clic su Salva e Continua.

5. Fare clic su Condizione per selezionare la macro che è possibile utilizzare per definire una condizione per questa regola. Eseguire una delle azioni seguenti per definire la condizione:

   Nota: una regola di notifica senza condizione invierà una notifica a tutti i contatti ogni volta che si verifica un'attività.

   - Cercare la macro nell'elenco e selezionarla.
   - Fare clic su Crea Nuovo per creare una macro.

6. Fare clic su Modello di messaggio per aggiungere un modello di messaggio che si è creato per questa regola. Effettuare una delle operazioni seguenti:

   - Cercare il modello nell'elenco e selezionarlo.
   - Fare clic su Crea Nuovo per creare un modello di messaggio.

7. Selezionare i contatti appropriati ai quali inviare la notifica dalle seguenti schede:

   Nota: Utilizzare il pulsante Aggiorna contatti visualizzato in ciascuna scheda per cercare e selezionare un numero maggiore di contatti a cui inviare la notifica.

   Contatti oggetto

Consente di visualizzare le organizzazioni, i vendor e gli elementi della configurazione disponibili per il tipo di oggetto selezionato che riceveranno la notifica sui ticket. Ad esempio, è possibile selezionare Utente finale interessato oppure Affected End User's Admin Org (Organizzazione dell'utente finale interessato) a cui inviare la notifica.

Contatti

Mostra le singole persone aggiunte alla regola di notifica, indipendentemente dalla loro associazione con il ticket.

Tipi contatto

Consente di visualizzare gli utenti che sono definiti all'interno della regola di notifica aventi la medesima classificazione, quali l'analista o il cliente.

8. Fare clic su Salva.

La regola di notifica viene creata.

Creazione di un'associazione attività

Associare un'attività con l'attributo oggetto per tenere traccia delle modifiche apportate all'attributo di oggetto relativo. Ad esempio, associare l'attività Aggiornamento campo con l'attributo oggetto del campo Descrizione di un record di incidente. Ciò consente di inviare una notifica ogni volta che la descrizione dell'incidente viene aggiornata. Un attributo oggetto può avere una sola notifica attività.

Nota: in caso di installazione dell'opzione multi-tenancy, selezionare il titolare appropriato dall'elenco a discesa. L'opzione pubblica (condivisa) consente di creare l'oggetto per tutti i titolari.

Procedere come descritto di seguito:

1. Selezionare Notifiche, Associazioni attività nella scheda Amministrazione.

   Viene visualizzata la pagina Elenco Associazioni attività.

2. Fare clic su Crea Nuovo.

   Viene visualizzata la pagina Crea Nuovo tipo di associazione attività.

3. Inserire i dati nei seguenti campi:

   Simbolo

   Definisce un identificatore univoco per questa associazione.

   Codice

   Definisce un codice interno per l'associazione attività.

   Tipo di oggetto

   Consente di specificare il nome dell'oggetto cui è possibile applicare l'attributo. Ad esempio, selezionare Richiesta / Incidente/ Problema.

   Attributo tipo oggetto

   Definisce l'attributo oggetto a cui è associato il tipo di attività. Ad esempio, immettere l'attributo oggetto del campo Descrizione di un record di incidente.

   Tipo attività

   Indica il tipo di attività. Ad esempio, selezionare Aggiornamento campo per verificare quando l'attributo oggetto viene aggiornato.

   Registrazione

   Determinare se questa associazione attività crea una voce di registro nel registro di audit.

4. Fare clic su Salva.

   Viene visualizzata la pagina Dettagli Tipo associazione attività.

5. Fare clic su Chiudi finestra.

   L'associazione attività viene creata.

Creazione di una notifica attività

Associare l'attività a una notifica. Quando l'attività ha luogo, la notifica associata viene inviata ai contatti selezionati.

Nota: in caso di installazione dell'opzione multi-tenancy, selezionare il titolare appropriato dall'elenco a discesa. L'opzione pubblica (condivisa) consente di creare l'oggetto per tutti i titolari. Non è possibile avere notifiche attività Notifica manuale diverse per titolare oppure copiare una notifica attività Notifica manuale.

Procedere come descritto di seguito:

1. Selezionare Notifiche, Notifiche attività nella scheda Amministrazione.

   Viene visualizzata la pagina Elenco Notifiche attività.

2. Fare clic su Crea Nuovo.

   Viene visualizzata la finestra Crea Nuova notifica attività.

3. Inserire i dati nei seguenti campi:

   Simbolo

   Definisce un identificatore univoco per la notifica attività.

   Codice

   Consente di definire il codice interno per la notifica attività.

   Attività valida per

   Specifica l'oggetto al quale si applica l'attività.

4. Fare clic su Salva e Continua.

   Viene visualizzata la pagina Aggiorna notifica attività.

5. Inserire i dati nei seguenti campi:

   Interna

   Consente di specificare se la notifica attività è disponibile ai dipendenti interni o visibile agli utenti finali.

   Stato record

   Specifica se la notifica attività è attualmente attiva o inattiva. Impostare lo stato su Attivo per utilizzare l'associazione attività.

Attività ticket correlato

Specifica se il registro delle attività di un ticket viene propagato a tutti i ticket correlati. Il registro attività può essere propagato solo per gli incidenti, i problemi e gli ordini di cambiamento correlati.

Nota: Se si usa la funzionalità di multi-tenancy, procedere come segue:

- Nell'elenco a discesa Attività ticket correlata, specificare il tipo di titolare appropriato.
- Immettere il nome del titolare nel campo del titolare o fare clic sull'icona di ricerca per individuarne uno.

Tipo di oggetto

Specifica il nome dell'oggetto a cui si applica l'attività.

6. Selezionare la scheda Regole di notifica e fare clic su Aggiorna regole di notifica. Eseguire una delle seguenti operazioni:
   - Immettere i criteri di ricerca, fare clic su Cerca e selezionare la regola di notifica tra i risultati della ricerca.
   - Fare clic su Crea Nuovo per creare una regola di notifica.

7. (Se si desidera inviare un questionario di indagine al destinatario della notifica) Selezionare la scheda Indagine e definire una notifica di indagine (a pagina 202). Le indagini consentono di raccogliere e analizzare il feedback dei clienti. Un registro attività viene generato sia quando una notifica indagine viene inviata sia quando ricevuta da un cliente.

   Nota: La scheda Indagine è applicabile a tutti i tipi di oggetto ad eccezione di Documenti della conoscenza, Commenti documento della conoscenza e Scheda report della conoscenza. Quando è specificata nell'elenco Tipo di oggetto, la scheda Posta elettronica viene visualizzata al posto della scheda Indagine nella pagina Aggiorna notifica attività. Dalla scheda Posta elettronica, è possibile ricercare uno o più messaggi di posta elettronica da associare a questa notifica o definirne uno nuovo.

8. (Se si desidera attivare un evento dopo l'invio della notifica) Selezionare la scheda Eventi. Gli eventi sono procedure attuate da un sistema di gestione delle questioni allo scadere di un periodo di tempo specificato. Quando la notifica di attività viene attivata, si verificano gli eventi selezionati. Ad esempio, aggiornare lo stato dell'incidente in Chiudi. Cercare l'evento e fare clic sul pulsante Aggiorna eventi per aggiungere l'evento a una notifica di attività.

9. Fare clic su Salva.

   Viene visualizzata la pagina Dettagli Notifiche attività.

10. Fare clic su Chiudi finestra.

    La notifica attività viene creata. Se si verifica un errore sul server di posta elettronica in uscita, le notifiche di posta elettronica non vengono inviate e vengono accodate nella directory $NX_ROOT/site/mail_queue. Quando il server di posta elettronica diventa nuovamente attivo, trascorso un intervallo di tempo, elabora e invia i messaggi di posta elettronica rimasti in coda. È possibile impostare la variabile dell'intervallo tra tentativi (a pagina 202) per riavviare i messaggi di posta elettronica accodati quando il server di posta elettronica era occupato.

    I messaggi di notifica non inviati dal server di posta elettronica in uscita vengono rinviati, salvo il caso in cui venga eseguita una delle seguenti operazioni:

    - Viene arrestato il componente Mail Daemon (pdm_mail_nxd) che gestisce le notifiche di posta elettronica in uscita.
    - Vengono eliminati manualmente i messaggi dalla directory %NX_ROOT%\site\mail_queue.

Definizione di notifiche di indagine.

Completare i campi seguenti in modo appropriato:

Invia l'indagine

Indica se attivare o disattivare l'indagine. Se selezionata, l'indagine viene inviata al contatto all'attivazione dell'attività di notifica selezionata.

Indagine predefinita

Specificare un'indagine predefinita utilizzando l'icona di ricerca o specificarne una propria nella casella di testo.

Titolo del messaggio indagine

Immettere il titolo dell'indagine.

Testo del messaggio indagine

Immettere un messaggio per il contatto. Quando un contatto riceve la notifica di un'indagine, il testo del messaggio include un URL al quale può accedere direttamente dal proprio browser Web per trovare e completare il modulo di indagine.

Impostazione della variabile dell'intervallo tentativi per la posta elettronica

È possibile definire l'intervallo di tempo (in secondi) tra i tentativi non riusciti di invio di messaggi di posta elettronica dal server di posta elettronica.

Nota: CA SDM non effettua tentativi di invio di messaggi che sono stati accettati dal server di posta elettronica in uscita ma che non sono stati recapitati. Per questi messaggi sono attive le funzionalità e le policy di ripetizione dei tentativi di invio posta elettronica del server di posta elettronica in uscita.

I tentativi sono per messaggio. Se il server di posta elettronica non è disponibile per un periodo, anziché inviare tutti i messaggi contemporaneamente, viene effettuato un tentativo di invio per ogni messaggio allo scadere del relativo intervallo. Tuttavia, se si riavvia il daemon della posta elettronica in uscita, il sistema tenta di inviare contemporaneamente tutti i messaggi non inviati, e se l'invio non riesce, vengono reimpostati contemporaneamente tutti gli intervalli tra tentativi per tutti i messaggi.

L'impostazione (NX_EMAIL_RETRY_INTERVAL) del file NX.env file controlla l'intervallo tra tentativi. È possibile modificare l'impostazione predefinita dell'intervallo tra tentativi su uno o più server.

Procedere come descritto di seguito:

1. Accedere al server seguente, a seconda della configurazione di CA SDM:
   - Convenzionale: server primario
   - Disponibilità avanzata: server in background.
2. Accesso alla directory $NX_ROOT
3. Aprire il file NX.env con un editor di testo, quale WordPad.
4. Modificare il valore dell'intervallo NX_EMAIL_RETRY_INTERVAL come indicato di seguito:

   ```
   NX_EMAIL_RETRY_INTERVAL=numero_di_secondi
   ```

   NX_EMAIL_RETRY_INTERVAL

   Definisce l'intervallo di tempo (in secondi) tra i tentativi non riusciti di invio di messaggi di posta elettronica.

   numero_di_secondi

   Specifica il numero di secondi per ogni intervallo tra tentativi. Il valore predefinito è 600 secondi (10 minuti). Il valore minimo consentito è 20 secondi. Se si imposta un valore inferiore a quello minimo di 20 secondi o superiore a quello massimo di 2000000 secondi, viene utilizzato il valore predefinito di 10 minuti.
5. Salvare e chiudere il file.
6. Riavviare i server di CA SDM. Per ulteriori informazioni su come avviare il server di CA SDM, a seconda della configurazione di CA SDM, consultare lo scenario *Riavvio dei server di CA SDM* o consultare le informazioni nella *Guida per l'amministratore*.

   Le modifiche diventano effettive.

Modalità di creazione di notifiche contatto oggetto

Le notifiche contatto oggetto consentono di inviare notifiche ai destinatari in base al valore corrente di un campo del ticket. Anziché identificare una persona a cui inviare la notifica, come accade con il metodo di notifica, è possibile identificare un oggetto. Ad esempio, è possibile identificare il campo A per garantire l'invio della notifica alla persona specificata nel campo A, anche se tale valore è stato modificato in seguito alla definizione del ticket.

Procedere come descritto di seguito:

1. Selezionare Notifiche, Notifiche contatto oggetto nella scheda Amministrazione.

   Viene visualizzata la pagina Elenco Notifiche contatto oggetto.
2. Fare clic su Crea nuovo.

   Viene visualizzata la pagina Crea Nuova notifica contatto oggetto.

3. Inserire i dati nei seguenti campi:

   Simbolo

   Consente di definire un identificatore univoco per la notifica contatto oggetto.

   Stato

   Consente di specificare se la notifica contatto oggetto è attualmente attiva o inattiva.

   Tipo di oggetto

   Consente di visualizzare il nome dell'oggetto cui è possibile applicare l'attributo.

   Nome attributo oggetto

   Consente di visualizzare il nome della notifica contatto oggetto (nel campo Simbolo) in Majic, ovvero nel codice CA interno. Il nome dell'attributo dipende dalla selezione del tipo di oggetto:

   - Se il tipo oggetto è Questione o Attività flusso di lavoro, il nome attributo è l'assegnatario, il richiedente o il gruppo; si tratta dei nomi attributo degli oggetti Cambiamento associati ai campi nelle tabelle Change_Request.
   - Se il tipo oggetto è Questione o Attività flusso di lavoro, il nome attributo è l'assegnatario, il richiedente o il gruppo; si tratta dei nomi attributo degli oggetti Cambiamento associati ai campi nelle tabelle Change_Request. Il nome attributo potrebbe essere change_id.group.

   Descrizione

   Descrive la notifica contatto oggetto.

4. Fare clic su Salva.

   La nuova notifica di contatto oggetto viene visualizzata in Elenco Notifiche contatto oggetto.

Nota: Per ulteriori informazioni sulla configurazione delle notifiche contatto oggetto, consultare la *Guida in linea*.

Elenco destinatari per notifica manuale

È possibile impostare un insieme predefinito di Destinatari disponibili che la pagina di composizione Notifica manuale presenta per richieste, incidenti e problemi. I Destinatari disponibili semplificano il processo di notifica manuale per gli analisti poiché è possibile impostare un elenco di oggetti contatto (ad esempio, Utente finale interessato) o di nomi di singoli contatti da utilizzare come destinatari di notifiche manuali.

Aggiungendo Destinatari Contatto oggetto, vengono aggiunti all'elenco Destinatari i nomi di singoli contatti che tale contatto oggetto rappresenta (consolidando eventuali voci duplicate). È possibile fare riferimento più volte allo stesso contatto per vari oggetti contatto, ad esempio come Assegnatario e Utente finale interessato. Alcune voci, quale l'oggetto contatto Elenco stakeholder, possono aggiungere più voci all'elenco Destinatari.

Contatti e oggetti contatto rimangono nell'elenco Destinatari disponibili dopo averli aggiunti all'elenco. Questo consente di rimuovere destinatari senza influire sull'elenco Destinatari disponibili.

Esempio: modalità di funzionamento dell'elenco Destinatari disponibili

Gli esempi riportati di seguito dimostrano come i destinatari predefiniti semplificano il processo di notifica manuale.

I Destinatari contatto oggetto includono le seguenti voci:

- UtenteA appartiene agli oggetti contatto "Assegnatario" e "Utente finale interessato".
- L'Elenco stakeholder include più nomi di contatto. Ad esempio, UtenteB e UtenteC.

È possibile eseguire le seguenti operazioni:

- Aggiungere entrambi gli oggetti contatto che si riferiscono all'UtenteA all'elenco Destinatari.

  Solo una voce UtenteA è elencata nell'elenco Destinatari.

- Rimuovere accidentalmente l'UtenteA dall'elenco Destinatari.

  Non è necessario fare riferimento al ticket per ottenere il nome dell'UtenteA e cercarlo per aggiungerlo nuovamente. È possibile aggiungere rapidamente l'UtenteA all'elenco Destinatari perché l'UtenteA è incluso nell'elenco Destinatari disponibili.

- Rimuovere accidentalmente un nome di contatto, ad esempio UtenteC, dall'elenco Destinatari proveniente dall'Elenco stakeholder.

  È possibile aggiungere l'Elenco stakeholder dai Destinatari contatto oggetto per aggiungere nuovamente il nome del contatto. Poiché le voci duplicate vengono consolidate, gli altri contatti dell'Elenco stakeholder che non sono stati eliminati dall'elenco Destinatari non hanno subito modifiche.

Notifiche assegnatario precedente

È possibile configurare i valori del gruppo o dell'assegnatario precedente per una notifica attività che rileverà i cambiamenti apportati ai campi chiave nel momento in cui viene salvato un ticket. I valori dell'assegnatario o del gruppo precedente consentono di notificare il trasferimento di un ticket ad un assegnatario precedente o di notificare l'escalation della priorità di un ticket sia al gruppo corrente che a quello precedente.

I campi di valori precedenti di un ticket sono campi locali presenti solo nella memoria e non nel database. I valori dei campi vengono inseriti durante l'operazione di salvataggio di un ticket e cancellati al completamento del processo di notifica. Il campo di un valore precedente viene associato ad un determinato tipo di attività tramite un'associazione attività.

È possibile definire i valori precedenti che rilevano le modifiche ai seguenti campi chiave di un ticket:

Campo	Richieste, Incidenti, Problemi	Ordini di cambiamento	Questioni
Stato	Sì	Sì	Sì
Attivo	Sì	Sì	Sì
Assegnatario	Sì	Sì	Sì
Area richiesta/Categoria richieste	Sì	Sì	Sì
Gruppo	Sì	Sì	Sì
Impatto	Sì	Sì	Sì
Priorità	Sì	Sì	Sì
Urgenza	Sì	No	No
Gravità	Sì	No	No

Per ogni tipo di oggetto, ovvero richiesta, incidente, problema, ordine di cambiamento o questione, è possibile specificare diversi contatti che notificano il verificarsi di un'attività ai contatti correnti e precedenti.

- **Assegnatario**: persona cui è assegnata la gestione del ticket.
- **Assegnatario precedente**: persona cui è stata precedentemente assegnata la gestione del ticket.
- **Gruppo**: gruppo cui è assegnata la gestione del ticket.
- **Gruppo precedente**: gruppo cui è stata precedentemente assegnata la gestione del ticket.

Dopo il salvataggio della regola di notifica, i campi Assegnatario precedente e Gruppo precedente vengono visualizzati nella pagina di elenco Notifiche contatto oggetto.

Esempio: Configurazione dei valori corrente e precedente dei campi chiave

Il seguente esempio di utilizzo descrive la procedura di configurazione, da parte di un amministratore, dei valori correnti e precedenti dei campi chiave per garantire l'invio della notifica di trasferimento di una Richiesta al rappresentante del supporto.

1. **Situazione**: un ticket viene trasferito ma il rappresentante del supporto non viene notificato.
2. **Attività**: l'amministratore aggiunge i contatti oggetto Assegnatario e Assegnatario precedente alla regola di notifica per la notifica dell'attività di trasferimento. Tali contatti associano un modello di messaggio e specificano gli assegnatari corrente e precedente cui inviare la notifica sul modulo di richiesta.
3. **Azione**: quando la richiesta viene salvata, vengono inseriti i valori nei campi Assegnatario e Assegnatario precedente della richiesta. Quando viene eseguita l'attività, ovvero il trasferimento del ticket, viene valutata la condizione della regola.
4. **Risultato**: se la condizione viene soddisfatta, viene inviato un messaggio di notifica che descrive l'attività del ticket all'assegnatario corrente e all'assegnatario precedente.

Esempio di notifica ai contatti del trasferimento di un ticket

È possibile notificare il trasferimento di un ticket CA SDM sia ai contatti correnti che a quelli precedenti.

Esempio: notifica del trasferimento di un ticket sia ai contatti correnti che a quelli precedenti

1. Nella scheda Amministrazione, accedere a Notifiche, Notifiche attività.

   Viene visualizzata la pagina Elenco notifiche attività.
2. Selezionare la notifica attività Trasferimento desiderata.

   Viene visualizzata la pagina Transfer Activity Notification Detail.
3. Nel campo di Tipo oggetto, selezionare Richieste/Incidenti/Problemi.
4. Nella scheda Regole di notifica, sotto Simbolo, selezionare Regola di notifica predefinita Trasferimento.

   Viene visualizzata la pagina Regola di notifica predefinita Trasferimento.
5. Nella scheda Contatti oggetto, fare clic su Aggiorna contatti oggetto.
6. Fare clic su Ricerca.

   Viene visualizzata la pagina Notification Rule Update Recipients.

7. Dall'elenco Contatti oggetto a sinistra selezionare Assegnatario e Assegnatario precedente, quindi fare clic sul pulsante di selezione del contatto (>>).

   L'elemento selezionato viene aggiunto all'elenco sulla destra.

   Nota: utilizzare il tasto CTRL o SHIFT oltre il pulsante sinistro del mouse per selezionare contatti oggetto multipli.

8. Fare clic su OK.

9. Salvare la regola di notifica.

   L'elenco Contatti oggetto visualizza il contatto oggetto selezionato.

10. Nella pagina Regola di notifica predefinita Trasferimento fare clic su Modello messaggio. Selezionare un modello e verificare che l'opzione Notifica automatica sia abilitata.

11. Creare una richiesta, specificare un assegnatario, quindi fare clic su Salva.

12. Nella pagina Dettagli richiesta selezionare Attività e successivamente Trasferimento dal menu File.

13. Specificare un nuovo assegnatario e fare clic su Salva.

    La notifica viene inviata agli assegnatari correnti e precedenti nel momento in cui si è verificata l'attività di trasferimento.

Notifiche elemento della configurazione

Una notifica elemento della configurazione consente di definire una notifica attività associata ad un elemento della configurazione specifico associato ad un ticket CA SDM specifico. Questa funzione consente di tenere traccia delle informazioni sugli utenti, sulle organizzazioni e sui vendor di un elemento della configurazione.

È possibile specificare i contatti oggetto elementi della configurazione nella pagina dei destinatari dell'aggiornamento regole di notifica, quali Organizzazione manutenzione elementi della configurazione, Contatto primario per gli elementi della configurazione e così via.

Esempio di notifica al contatto primario di un elemento della configurazione per una questione

È possibile definire una notifica attività per un contatto primario da inviare per un elemento della configurazione specifico di un determinato ticket CA SDM.

Esempio: notifica al contatto primario di un elemento per una questione

1. Nella scheda Amministrazione, accedere a Notifiche, Notifiche attività.

   Viene visualizzata la pagina Elenco notifiche attività.

2. Selezionare la notifica attività Iniziale dall'elenco.

   Viene visualizzata la pagina Dettagli notifica attività iniziale.

3. Selezionare il tipo di oggetto che si desidera utilizzare:
4. Nella scheda Regole di notifica selezionare il collegamento Regola di notifica predefinita.

   Viene visualizzata la pagina Regola di notifica predefinita.
5. Selezionare il collegamento Modello messaggio predefinito e verificare che sia abilitata l'opzione Notifica automatica.
6. Selezionare la scheda Contatti oggetto e fare clic su Aggiorna contatti oggetto.

   Viene visualizzata la pagina Ricerca notifiche contatto oggetto.
7. Fare clic su Ricerca. Viene visualizzato un elenco dei contatti oggetto.
8. Selezionare il contatto primario dell'elemento della configurazione dall'elenco a sinistra e fare clic sul pulsante di selezione del contatto (>>).

   L'elemento selezionato viene aggiunto all'elenco sulla destra.

   È possibile utilizzare anche il tasto CTRL o MAIUSC e il pulsante sinistro del mouse per selezionare contatti oggetto multipli. È possibile aggiungere un oggetto per una richiesta e diversi oggetti per un ordine di cambiamento o una questione.

   Il contatto oggetto si trova nell'elenco a destra.
9. Fare clic su OK.
10. Salvare la regola di notifica.

    L'elenco Contatti oggetto visualizza il contatto oggetto selezionato.
11. Completare le seguenti attività:
    - Nella scheda Service Desk creare o aggiornare un elemento della configurazione esistente.
    - Aggiungere il contatto principale in elenco nella scheda Contatti oggetto. Il contatto oggetto selezionato appare nella pagina Dettagli elementi della configurazione.
    - Aggiungere l'elemento della configurazione alla questione.

Quando si verifica un evento attività, viene implementata la regola e viene valutata la condizione. Se vengono soddisfatti i criteri della condizione, viene inviato un messaggio di notifica che descrive l'attività del ticket a tutti i contatti dell'elemento della configurazione associato a questa regola di notifica.

Lettore registro notifiche

Lettore registro notifiche visualizza le notifiche ricevute dall'utente collegato in base a data, urgenza e stato. Con Lettore registro notifiche è possibile eseguire le seguenti operazioni:

- Modificare l'ordinamento e impostare le opzioni di menu affinché Lettore registro notifiche venga visualizzato non appena vengono ricevuti nuovi messaggi.

- Fare doppio clic su un messaggio di notifica per richiedere che CA SDM visualizzi la pagina dei dettagli del ticket associato alla notifica.
- Monitorare i messaggi di notifica immettendo criteri di selezione specifici per eseguire query nel database relativamente ad analisi o alla selezione dei messaggi di notifica in base ai dati immessi nei campi. Ad esempio, è possibile elencare solo i messaggi di notifica che non sono stati cancellati, impostando il campo Stato messaggio su Non cancellato.
- Cancellare i messaggi di notifica per mantenere l'elenco delle notifiche di dimensioni gestibili. Le notifiche cancellate non vengono visualizzate quando si accede per la prima volta a Lettore registro notifiche, sebbene, se necessario, sia possibile visualizzarle.

Impostazione delle opzioni di Lettore registro notifiche

È possibile impostare le opzioni di Lettore registro notifiche per definire in che modo essere avvisati quando si ricevono nuovi messaggi per una questione.

Per impostare le opzioni di Lettore registro notifiche

1. Nella scheda ServiceDesk accedere a Visualizza, Lettore registro.

   Viene visualizzata la pagina Lettore registro notifiche.

2. Utilizzare la casella di controllo a sinistra di ogni notifica per impostare le seguenti opzioni. Si possono selezionare diverse voci per eseguire operazioni come Deseleziona selezione o Elimina selezione.

   Intestazione

   Visualizza l'intestazione del messaggio, in genere contenente il numero del ticket e il tipo di attività.

   Data inizio

   Consente di visualizzare la data e l'ora di invio della notifica alla finestra Lettore registro.

   Stato

   Visualizza lo stato della notifica.

   Urgenza

   Definisce il livello di urgenza della notifica (basso, medio, alto o emergenza), che indica l'importanza relativa di differenti attività. I livelli di urgenza sono predefiniti; tuttavia, l'amministratore del sistema è responsabile della configurazione di altri aspetti della notifica, quali i metodi di notifica e le associazioni di attività. L'amministratore del sistema definisce inoltre il metodo di notifica utilizzato per i contatti e i gruppi per ciascun livello di urgenza.

Testo del messaggio

Si tratta del testo completo del messaggio di notifica.

Il Lettore registro mostra tutti i cambiamenti.

3. Fare clic su Chiudi.

   La pagina Lettore registro notifiche viene chiusa e le opzioni vengono impostate.

Risposte personalizzate

È possibile creare risposte personalizzate ed allegarle alle richieste, questioni e ai record degli ordini di cambiamento quando si aggiungono le attività al record. È possibile, ad esempio, aggiungere risposte personalizzate alle finestre Modifica stato o Registra commento disponibili nel menu Attività.

Creazione di una risposta personalizzata

È possibile creare una risposta personalizzata da aggiungere a richieste, questioni e record di ordini di cambiamento.

Per creare una risposta personalizzata

1. Dalla scheda Amministrazione, accedere a Service Desk, Risposte personali.

   Viene visualizzata la pagina dell'elenco delle risposte personali.

2. Fare clic su Crea nuovo.

   Viene visualizzata la pagina Crea nuova risposta personalizzata.

3. Completare i campi nella pagina.

   Proprietario risposta

   Specifica il contatto proprietario della risposta. Se questo valore è lasciato vuoto, la risposta è disponibile per tutti gli analisti.

   Risposta

   Specifica il testo inviato a tutti coloro che ricevono questa risposta. Questo campo può contenere fino a 1000 caratteri.

   È possibile utilizzare variabili come:

```
Ticket ref_num: @{call_req_id.ref_num}
Assegnatario: @{call_req_id.assignee.combo_name}
Cliente: @{call_req_id.customer.combo_name}
Descrizione: @{call_req_id.description}
```

4. Selezionare i tipi di record per i quali si desidera rendere disponibile la risposta. Fare clic su Salva.

   Viene creata una risposta personalizzata.

Sostituzione di variabili di risposta personalizzata

È possibile includere variabili nel testo di una risposta personale. Queste variabili consentono di sostituire informazioni provenienti dalla Richiesta, dall'Ordine di cambiamento, dalla Issue, dal Problema o dall'Incidente corrispondente. La sintassi delle variabili è la stessa utilizzata in altri contesti del prodotto CA SDM, ad esempio nei modelli dei messaggi di notifica di un'attività e nel testo del messaggio dell'attività di notifica manuale. È possibile sostituire solo le informazioni provenienti dalla Richiesta, dall'Ordine di cambiamento, dalla Issue, dal Problema o dall'Incidente corrispondente. I modelli dei messaggi di notifica di un'attività e il testo del messaggio dell'attività di notifica manuale permettono di includere anche informazioni provenienti dal record di un registro attività.

Le caselle di controllo relative ad ogni tipo di oggetto (Richieste, Ordini di cambiamento, Issue, Incidenti e Problemi) consentono di filtrare le risposte durante la fase di selezione. Se il tipo di oggetto non è selezionato, la rispettiva risposta non sarà disponibile. Se ad esempio è selezionata solo la casella Richiesta, la risposta verrà presentata solo in Attività per la richiesta.

È possibile utilizzare un'unica risposta per tutti i tipi di oggetti (Richieste, Ordini di cambiamento, Issue, Problemi o Incidenti). Poiché ogni oggetto presenta diversi attributi, le informazioni non relative all'oggetto non vengono sostituite, ad esempio tentando di sostituire il numero di Richiesta in una risposta relativa ad una Issue.

Di seguito sono riportati un esempio di testo della risposta e le sostituzioni di variabili che si verificano per ogni tipo di oggetto:

```
Questo è il N. Richiesta '@{call_req_id.ref_num}'
Questo è il N. Ordine di cambiamento '@{change_id.chg_ref_num}'
Questo è il N. Issue '@{issue_id.ref_num}'
```

Per una *Richiesta* si verifica la seguente sostituzione:

```
Questo è il N. Richiesta 'cr_demo:11'
Questo è il N. Ordine di cambiamento "
Questo è il N. Issue "
```

Per un *Ordine di cambiamento* si verifica la seguente sostituzione:

```
Questo è il N. Richiesta "
Questo è il N. Ordine di cambiamento 'chg_demo:3'
Questo è il N. Issue "
```

Per una *Issue* si verifica la seguente sostituzione:

```
Questo è il N. Richiesta "
Questo è il N. Ordine di cambiamento "
Questo è il N. Issue n. 'iss_demo:6'
```

Se si utilizzano le caselle di controllo "Visualizza questa risposta per", è possibile creare diverse versioni di una risposta mediante le variabili di sostituzione appropriate per l'oggetto corrispondente (Richieste, Ordini di cambiamento, Issue, Problemi o Incidenti).

Il formato delle variabili di sostituzione per i diversi oggetti è il seguente.

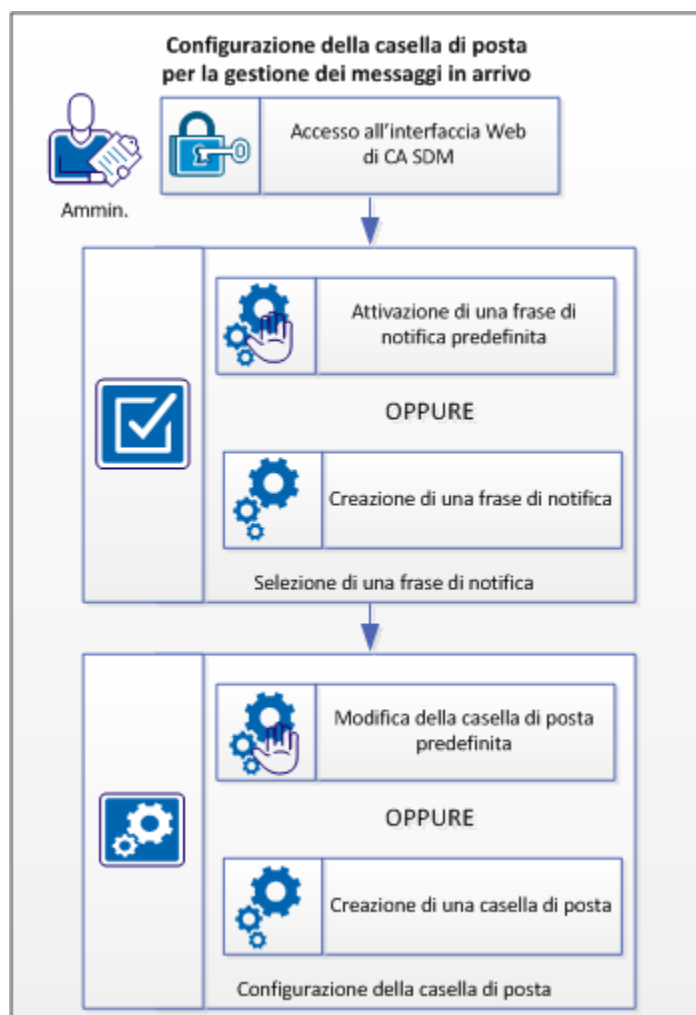
Oggetto	Formato delle variabili
Richiesta/Incidente/Problema	@{call_req_id.attr}
Ordine di cambiamento	@{change_id.attr}
Issue	@{issue_id.attr}

La sostituzione avviene quando si copia la risposta nel campo Descrizione utente. La risposta viene copiata dopo che è stata selezionata dall'elenco a discesa Risposta personalizzata. L'elenco perde quindi lo stato attivo.

Modalità di configurazione della casella di posta per la gestione dei messaggi di posta elettronica in entrata

La posta elettronica consente di comunicare con utenti finali, quali dipendenti o clienti. La casella di posta di CA SDM gestisce i messaggi di posta elettronica in entrata degli utenti ed esegue un'azione in base al messaggio. Ad esempio, l'utente invia un messaggio di posta elettronica a CA SDM per creare un incidente. La casella di posta verifica il messaggio, crea un incidente e invia una notifica all'utente informandolo che l'incidente è stato creato correttamente.

CA SDM fornisce una casella di posta predefinita (denominata Predefinito) che è attiva e che può essere utilizzata dall'organizzazione. È possibile modificare la casella di posta predefinita, creare caselle di posta aggiuntive o effettuare entrambe le operazioni. Dopo avere creato una casella di posta o avere modificato una casella di posta predefinita, se ne definiscono le regole. Le regole della casella di posta consentono di configurare le azioni, le risposte, o entrambe, per i messaggi recuperati da una casella di posta.

Il diagramma seguente mostra come configurare la casella di posta per gestire i messaggi di posta elettronica in entrata:

Procedere come descritto di seguito:

1. Aprire l'interfaccia utente Web di CA SDM (a pagina 191).
2. Scegliere una frase di notifica (a pagina 215).
   - Attivare una frase di notifica predefinita (a pagina 216).
   - Creare una frase di notifica (a pagina 217).
3. Configurare la casella di posta (a pagina 223).
   - Modificare la casella di posta predefinita (a pagina 223).
   - Creare una casella di posta (a pagina 228).

Apertura dell'interfaccia utente Web di CA SDM

Accedere all'interfaccia utente Web dai server seguenti, in base alla configurazione di CA SDM:

- Convenzionale: server primario o secondario
- Disponibilità avanzata: server applicazioni o in background

Scelta di una frase di notifica

La frase di notifica viene inviata al mittente del messaggio di posta elettronica. Ad esempio, per confermare che un Incidente è stato creato correttamente. CA SDM fornisce frasi di notifica predefinite che vengono impostate come inattive per impostazione predefinita. È possibile attivare e modificare le frasi. È possibile inoltre creare frasi di notifica in base alle esigenze della propria organizzazione.

Scegliere una delle seguenti opzioni:

- Attivare una frase di notifica predefinita (a pagina 216).
- Creazione di una frase di notifica (a pagina 217)

Attivazione di una frase di notifica predefinita

Per impostazione predefinita, le frasi di notifica predefinite sono inattive. È possibile attivare una frase di notifica in modo che la frase venga utilizzata dalle notifiche.

Nota:se Multi-Tenancy è installato, selezionare un titolare dall'elenco a discesa. L'opzione pubblica (condivisa) consente di creare l'oggetto per tutti i titolari.

Procedere come descritto di seguito:

1. Selezionare Notifiche, Frasi di notifica nella scheda Amministrazione.

   Viene visualizzata la pagina Elenco Frasi di notifica.

2. Cercare la frase di notifica.

3. Fare clic sulla frase che si desidera attivare. Ad esempio, selezionare Cronologia notifiche - Cambiamento.

   Viene visualizzata la pagina Dettagli frase di notifica.

4. Fare clic su Modifica.

   Viene visualizzata la pagina Aggiorna frase di notifica.

5. Selezionare Attivo dall'elenco a discesa Attivo.

6. (Facoltativo) Modificare gli altri campi (a pagina 217), se necessario. Ad esempio, modificare la frase.

7. Fare clic su Salva.

   Viene visualizzata la pagina Dettagli frase di notifica.

8. Fare clic su Chiudi finestra.

   La frase di notifica è attiva.

Creazione di una frase di notifica

È possibile creare una frase di notifica che contenga testo standardizzato e macro. Questa frase di notifica viene inviata come risposta ai messaggi di posta elettronica degli utenti.

Nota:se Multi-Tenancy è installato, selezionare un titolare dall'elenco a discesa. L'opzione pubblica (condivisa) consente di creare l'oggetto per tutti i titolari.

Procedere come descritto di seguito:

1. Selezionare Notifiche, Frasi di notifica nella scheda Amministrazione.

   Viene visualizzata la pagina Elenco Frasi di notifica.

2. Fare clic su Crea Nuovo.

   Viene visualizzata la pagina Crea Nuova frase di notifica.

3. Compilare i campi della frase di notifica (a pagina 217) in base alle proprie esigenze.

4. Fare clic su Salva.

   La frase di notifica viene creata.

Campi della frase di notifica

Completare i campi seguenti per modificare o creare una frase di notifica:

Simbolo

Consente di definire un identificatore univoco per questo record.

Codice

Specifica un valore univoco da utilizzare per la frase di notifica, nella tabella usp_notification_phrase. Nella tabella usp_notification_phrase sono elencate frasi comuni che è possibile utilizzare nei modelli di messaggio di notifica. Per informazioni sulla tabella usp_notification_phrase, consultare la *Guida di riferimento tecnico*.

Frase

Specifica la frase per la notifica. È possibile specificare sia una versione con testo semplice sia una versione HTML. HTML consolida la maggior parte dei caratteri di spazio in spazi singoli ed è quindi necessario specificare le interruzioni di riga e paragrafo utilizzando dei tag.

Ad esempio, la frase di testo semplice seguente viene utilizzata nella frase di notifica Notifica confidenziale:

```
Il presente messaggio di posta e ogni eventuale documento allegato ha
carattere riservato e ad esclusivo utilizzo del destinatario in indirizzo.
Ogni eventuale modifica, utilizzo, accesso o distribuzione da parte di
chiunque altro sarà ritenuto illegale. Qualora il presente messaggio fosse
stato ricevuto per errore, si prega di eliminarlo unitamente ad ogni eventuale
documento allegato avvertendo immediatamente il mittente.
```

È possibile utilizzare la frase HTML seguente per chiedere all'utente di visualizzare l'elenco delle notifiche:

```
Fare clic sull'URL seguente per visualizzare l'elenco delle notifiche:
@{call_req_id.web_url}+HTMPL=cr_lr.htmpl+INSTANCE=@{id}
```

Per ulteriori informazioni sulle frasi, consultare l'argomento Codici e frasi di notifica (a pagina 218).

Frasi e codici di notifica

Le frasi di notifica consentono di aggiungere informazioni o testo standardizzato a più messaggi di notifica diversi, senza dover immettere e gestire il testo o formularlo separatamente per ogni modello di notifica. Ad esempio:

Rispondere a questa notifica per aggiungere informazioni aggiuntive al ticket

Le frasi standardizzano il testo da utilizzare in più modelli di messaggio. Ad esempio, è possibile gestire una frase comune, ad esempio una notifica confidenziale, in un solo record e utilizzarla in più modelli di messaggio. Le frasi di notifica sono inoltre utili per le risposte a messaggi, ad esempio una notifica di risposta o un URL Web. In CA SDM sono disponibili frasi di notifica predefinite ed è inoltre possibile creare frasi personalizzate. È possibile impostare una frase come attiva o non attiva per l'uso globale in un modello di messaggio. Le frasi di notifica sono disattive per impostazione predefinita. Quando una frase è disattiva, viene soppressa in tutti i modelli di messaggio che la utilizzano.

È inoltre possibile utilizzare le frasi di notifica nelle risposte automatiche a messaggi di posta elettronica in entrata. Il contesto di elaborazione di questo tipo di messaggio è tuttavia diverso. Omettere il prefisso (change_id., issue_id., call_req_id.) utilizzato in determinate macro quali ref_num e web_url per frasi utilizzate dal messaggio. Ne consegue che non è possibile condividere frasi di notifica tra modelli di notifica e risposte automatiche a messaggi di posta elettronica.

Di seguito sono ad esempio elencate alcune frasi predefinite fornite da CA SDM:

Simbolo	Codice	Frase
Cronologia notifiche - Cambiamento	notify_history_chg	Fare clic sull'URL seguente per visualizzare l'elenco Notifiche: @{change_id.web_url}+HTMPL=chg_lr.htmpl+INSTANCE=@{id}
Cronologia notifiche - Questione	notify_history_iss	Fare clic sull'URL seguente per visualizzare l'elenco Notifiche: @{issue_id.web_url}+HTMPL=iss_lr.htmpl+INSTANCE=@{id}
Cronologia notifiche - Richiesta/Incidente/Problema	notify_history_cr	Fare clic sull'URL seguente per visualizzare l'elenco Notifiche: @{call_req_id.web_url}+HTMPL=cr_lr.htmpl+INSTANCE=@{id}

Esempi: nuove frasi

Di seguito sono riportati alcuni esempi di nuove possibili frasi:

Simbolo	Codice	Frase
Notifica di riservatezza	ConfidentialNotice	Il presente messaggio di posta e ogni eventuale documento allegato ha carattere riservato e ad esclusivo utilizzo del destinatario in indirizzo. Ogni eventuale modifica, utilizzo, accesso o distribuzione da parte di chiunque altro sarà ritenuto illegale. Qualora il presente messaggio fosse stato ricevuto per errore, si prega di eliminarlo unitamente ad ogni eventuale documento allegato avvertendo immediatamente il mittente.
Notifica di risposta a incidente	IncidentReply	Per aggiungere un commento all'incidente, è sufficiente rispondere a questo messaggio di posta elettronica o includere la riga seguente (in una riga autonoma). %incident_id=@{call_req_id.ref_num}
Notifica di URL incidente	IncidentURL	Fare clic sull'URL seguente per visualizzare: @{call_req_id.web_url}

Nota: utilizzare frasi separate per le versioni in formato testo normale e HTML dei modelli di messaggio o delle risposte automatiche a messaggi di posta elettronica. Il formato HTML consolida la maggioranza degli spazi in spazi singoli, pertanto è necessario specificare le interruzioni di riga o di paragrafo mediante tag. I tag HTML inclusi nelle versioni in formato testo normale dei messaggi vengono visualizzati anziché venire elaborati.

Sintassi delle frasi di notifica

Le frasi di notifica vengono inserite in modelli di messaggio e messaggi di posta elettronica di risposta in base alla seguente sintassi macro:

```
@{notification_phrase[codice].phrase}
```

codice

Specifica il valore Codice univoco, quale ConfidentialNotice, della tabella delle frasi dei messaggi (usp_notification_phrase).

Nota: la tabella usp_notification_phrase elenca frasi comuni che possono essere utilizzate nei modelli di messaggio di notifica. Per informazioni sulla tabella usp_notification_phrase, consultare la *Guida di riferimento tecnico*.

Ad esempio:

```
@{notification_phrase[IncidentURL1].phrase}
```

```
@{notification_phrase[RequestReply].phrase}
```

Quando la macro viene individuata, il testo della frase della tabella usp_notification_phrase sostituisce la sintassi. Se non esiste un codice corrispondente (oppure se non è attivo), la macro viene sostituita da una stringa vuota. Nel registro standard (STDLOG) non vengono scritti errori, ma viene registrato un messaggio di avviso per facilitare la risoluzione di potenziali problemi.

Nota: L'integrazione di frasi in altre frasi è limitato a un valore di profondità massimo configurato dall'impostazione della variabile di ambiente (a pagina 476) NX_MAX_EXPAND_DEPTH. Questa limitazione impedisce che si verifichino problemi dovuti all'elaborazione di frasi che fanno accidentalmente riferimento a se stesse (incorporano se stesse) o con un riferimento circolare (quando una frase incorpora una frase in cui è incorporata).

Esempio: Modalità di visualizzazione delle frasi di notifica in un messaggio

L'esempio riportato di seguito mostra come appaiono le frasi di notifica in un messaggio di notifica. L'esempio utilizza i seguenti codici e frasi:

Codice	Frase
ConfidentialNotice	Il presente messaggio di posta e ogni eventuale documento allegato ha carattere riservato e ad esclusivo utilizzo del destinatario in indirizzo. Ogni eventuale modifica, utilizzo, accesso o distribuzione da parte di chiunque altro sarà ritenuto illegale. Qualora il presente messaggio fosse stato ricevuto per errore, si prega di eliminarlo unitamente ad ogni eventuale documento allegato avvertendo immediatamente il mittente.
IncidentReply	Per aggiungere un commento all'Incidente, rispondere a questo messaggio oppure includere il seguente testo in una linea a parte. %incident_id=@{call_req_id.ref_num}
IncidentURL	Fare clic sull'URL seguente per visualizzare: @{call_req_id.web_url}

Il seguente modello di messaggio incluse le frasi di notifica:

```
@{call_req_id.type.sym} @{call_req_id.ref_num} chiuso.
Assegnato a: @{call_req_id.assignee.combo_name}
Cliente: @{call_req_id.customer.combo_name}
Descrizione: @{call_req_id.description}

@{notification_phrase[IncidentURL].phrase}
@{notification_phrase[IncidentReply].phrase}

@{notification_phrase[ConfidentialNotice].phrase}
```

Le frasi appaiono nel messaggio come riportato di seguito:

```
Incidente 1234 chiuso.
Assegnato a: Analyst, Joe
Cliente: Doe, John
Descrizione: descrizione del problema

Fare clic sull'URL seguente per visualizzare:
http://helpdesk/CAisd/pdmweb.exe?OP=SEARCH+FACTORY=chg+SKIPLIST=1+QBE.EQ.id=40072
3

Per aggiungere un commento all'Incidente, rispondere a questo messaggio oppure
includere il seguente testo in una linea a parte.
%incident_id=1234

Il presente messaggio di posta e ogni eventuale documento allegato ha carattere
riservato e ad esclusivo utilizzo del destinatario in indirizzo. Ogni eventuale
modifica, utilizzo, accesso o distribuzione da parte di chiunque altro sarà ritenuto
illegale. Qualora il presente messaggio fosse stato ricevuto per errore, si prega di
eliminarlo unitamente ad ogni eventuale documento allegato avvertendo immediatamente
il mittente.
```

Configurazione della casella di posta

CA SDM fornisce una casella di posta predefinita per connettersi al server di posta. È possibile configurare questa casella di posta predefinita per modificare la password, il nome utente, il nome host eccetera. È possibile creare anche caselle di posta aggiuntive per rispondere alle esigenze della propria organizzazione. Ogni casella di posta può avere la sua definizione, anziché utilizzare un unico insieme globale di definizioni. È possibile definire più caselle di posta e utilizzare modelli o valori predefiniti diversi per ogni casella di posta. Definizioni multiple consentono a singoli titolari di utilizzare caselle di posta separate oppure a un singolo titolare o a un'organizzazione di utilizzare più caselle di posta e ottenere comportamenti diversi per ognuna di esse.

Scegliere una delle possibilità seguenti o entrambe:

Importante: Si consiglia di impostare la casella di posta associata come non attiva prima di configurare una regola della casella di posta. Altrimenti eventuali messaggi recuperati dal server di posta elettronica nell'intervallo tra la prima e l'ultima modifica verranno elaborati utilizzando le regole attive in quel momento.

- Modificare la casella di posta predefinita (a pagina 223).
- Creare una casella di posta (a pagina 228).

Modifica della casella di posta predefinita

CA SDM fornisce una casella di posta predefinita attiva modificabile in base alle specifiche esigenze di recapito della posta elettronica dell'organizzazione.

Procedere come descritto di seguito:

1. Selezionare Posta Elettronica, Caselle di posta nella scheda Amministrazione.

   Viene visualizzata la pagina Elenco Caselle di posta.

2. Fare clic su Predefinito nella colonna Nome.

   Viene visualizzata la pagina Dettagli casella di posta predefinita.

3. Fare clic su Modifica.

4. Compilare o aggiornare gli altri campi in base alle proprie esigenze:

   Intervallo di controllo

   Specifica l'intervallo dopo il quale il server di posta viene controllato per la presenza di nuovi messaggi di posta elettronica.

   Attivo

   Indica lo stato della casella di posta.

   Tipo di messaggio di posta elettronica

   Specifica il protocollo utilizzato dal server di posta. CA SDM supporta sia POP3 sia IMAP4. Se si seleziona IMAP4, CA SDM controlla solo la cartella della posta in arrivo nella casella di posta.

   Nome host

   Specifica il nome host del server di posta elettronica.

   Ignora porta

   Specifica il numero di porta quando quello della porta predefinita viene ignorato.

   Nome utente

   Specifica l'ID utente sul server di posta.

   Password

   Specifica la password sul server di posta.

   Livello di protezione

   Specifica il livello di protezione SMTP.

   Repository allegati

   Specifica il repository in cui vengono archiviati gli allegati di posta elettronica.

   Allega intero messaggio di posta elettronica

   Specifica se usare l'intero messaggio di posta elettronica come allegato.

   Imponi separazione degli allegati

   Specifica se suddividere tutti gli allegati al messaggio di posta elettronica quando un intero messaggio di posta elettronica viene aggiunto come allegato. Il messaggio di posta elettronica e gli allegati vengono suddivisi in file separati e associati ai ticket. Applicabile solo quando è selezionata l'opzione Allega intero messaggio di posta elettronica.

   Consenti anonimo

   Specifica se è possibile creare i ticket da messaggi di posta anonimi.

   Salva messaggi di posta elettronica sconosciuti

Specifica se salvare i messaggi di posta elettronica non elaborati dalla regole definite nella casella di posta. Questi messaggi di posta elettronica vengono archiviati in $NX_ROOT/site/mail_unknown.

Usa indirizzo per le risposte

Specifica se utilizzare l'indirizzo di posta elettronica alternativo per le risposte.

Usa crittografia TLS

Specifica se utilizzare supporto Transport Layer Security (TLS) nei messaggi di posta elettronica.

Percorso certificato dell'autorità di certificazione

Specifica il percorso in cui è stato distribuito il certificato attendibile.

Nota: Per la configurazione con disponibilità avanzata, verificare di aver distribuito il certificato attendibile nella stessa posizione per i server in background e di standby. CA SDM supporta solo il formato di codifica in Base 64 (PEM) per i certificati dell'autorità di certificazione.

5. (Facoltativo) Creare o aggiornare le regole (a pagina 234) e le policy della casella di posta (a pagina 233) secondo necessità.

   Nota: Le regole applicabili a una casella di posta non possono essere associate a un'altra casella. Per riutilizzare le stesse regole per una casella di posta diversa, ricrearle per l'altra casella. È possibile anche copiare la casella di posta esistente.

   Importante: Si consiglia di impostare la casella di posta associata come non attiva prima di configurare una regola della casella di posta. Altrimenti eventuali messaggi recuperati dal server di posta nell'intervallo tra la prima e l'ultima modifica verranno elaborati utilizzando le regole attive.

6. Fare clic su Salva.

   Le modifiche apportate alla casella di posta predefinita vengono salvate e applicate. Il primo polling si verifica dopo un secondo.

Caselle di posta multiple

CA SDM può elaborare e gestire più caselle di posta. Ogni casella di posta può avere la sua definizione, anziché utilizzare un unico insieme globale di definizioni. È possibile definire più caselle di posta e utilizzare modelli o valori predefiniti diversi per ogni casella di posta. Definizioni multiple consentono a singoli titolari di utilizzare caselle di posta separate oppure a un singolo titolare o a un'organizzazione di utilizzare più caselle di posta e ottenere comportamenti diversi per ognuna di esse. È possibile impostare caselle di posta multiple tramite l'interfaccia di amministrazione. Ogni casella di posta utilizza le seguenti tabelle:

- usp_mailbox—Definisce la casella di posta.

- usp_mailbox_rule—Specifica un insieme di regole per ogni casella di posta.

  Poiché le regole della casella di posta forniscono i valori predefiniti all'interfaccia API testo, è possibile stabilire interfacce di posta elettronica con altri software e parametri (ad esempio, categoria, assegnatario e così via) configurati specificamente per l'interfaccia.

Nota: i server IMAP supportano caselle di posta multiple per un singolo account, ma non sono supportate caselle di posta alternative; è supportata solo la casella di posta predefinita.

Modalità di utilizzo delle regole da parte di caselle di posta multiple

Il daemon Mail Eater (pdm_maileater_nxd) sul server principale utilizza connessioni e regole di caselle di posta per leggere ed elaborare messaggi da uno o più account su uno o più server di posta elettronica. Il daemon Mail Eater elabora serialmente le caselle di posta (viene elaborata una sola casella di posta per volta) ed elabora le regole in sequenza.

Più caselle di posta utilizzano le regole come riportato di seguito:

1. All'avvio del server principale, il daemon Mail Eater legge le seguenti tabelle:

   usp_mailbox

   Rappresenta una connessione a un server di posta elettronica.

   usp_mailbox_rules

   Rappresenta le regole che si applicano alla connessione (usp_mailbox).

   Contact_Method

   Rappresenta i metodi di contatto utilizzati per le risposte automatiche.

   Document_Repository

   Rappresenta i repository documenti utilizzati per l'archiviazione degli allegati.

   Il daemon Mail Eater rileva automaticamente eventuali modifiche apportate agli oggetti in ognuna di queste tabelle, inclusa l'aggiunta di ulteriori oggetti. Se viene apportata una modifica alla tabella a usp_mailbox o usp_mailbox_rule, l'intervallo di polling delle caselle di posta interessate viene ripianificato a un secondo dopo l'applicazione della modifica.

2. In base all'intervallo definito per ogni casella di posta, il daemon Mail Eater recupera tutti i messaggi nella cartella della posta in arrivo per l'account associato ed elabora i messaggi come segue:

   a. Verifica l'indirizzo di posta elettronica per eventuali violazioni di norme. Se riscontra una violazione, l'elaborazione si arresta e viene coinvolto il registro standard in base alla definizione della casella di posta.

   b. Confronta il messaggio di posta elettronica con ogni regola (mailbox_rule) che appartiene a tale casella di posta.

c. Se trova una regola corrispondente, invia il messaggio all'interfaccia API testo per la registrazione e risponde all'utente come necessario in base all'azione specificata per la regola.

   Per i messaggi di risposta, la stringa di filtro identifica l'oggetto e utilizza l'interfaccia API testo per l'elaborazione. Al termine dell'elaborazione, la risposta viene inviata all'indirizzo Rispondi a oppure Da.

d. Dopo che il daemon Mail Eater ha trovato una regola corrispondente, non vengono controllate altre regole e viene elaborato il successivo messaggio nella cartella della posta in arrivo.

e. Se non vengono trovate regole corrispondenti, il messaggio viene scartato.

3. Dopo che il daemon Mail Eater ha elaborato tutti i messaggi di una cartella di posta in arrivo, i messaggi elaborati e quelli scartati vengono eliminati dal server di posta elettronica e viene pianificato il successivo intervallo di elaborazione.

Creazione di una casella di posta

È possibile creare una casella di posta che si connetta al server di posta e configurare i valori per l'host, l'utente, la password, ecc.

Procedere come descritto di seguito:

1. Selezionare Posta Elettronica, Caselle di posta nella scheda Amministrazione.

   Viene visualizzata la pagina Elenco Caselle di posta.

2. Fare clic su Crea Nuovo.

   Viene visualizzata la pagina Dettagli casella di posta.

3. Compilare i campi in modo appropriato:

   Intervallo di controllo

   Specifica l'intervallo dopo il quale il server di posta viene controllato per la presenza di nuovi messaggi di posta elettronica.

   Attivo

   Indica lo stato della casella di posta.

   Tipo di messaggio di posta elettronica

   Specifica il protocollo utilizzato dal server di posta. CA SDM supporta sia POP3 sia IMAP4. Se si seleziona IMAP4, CA SDM controlla solo la cartella della posta in arrivo nella casella di posta.

   Nome host

   Specifica il nome host del server di posta elettronica.

   Ignora porta

   Specifica il numero di porta quando quello della porta predefinita viene ignorato.

   Nome utente

   Specifica l'ID utente sul server di posta.

   Password

   Specifica la password sul server di posta.

   Livello di protezione

   Specifica il livello di protezione SMTP.

   Repository allegati

   Specifica il repository in cui vengono archiviati gli allegati di posta elettronica.

   Allega intero messaggio di posta elettronica

   Specifica se usare l'intero messaggio di posta elettronica come allegato.

   Imponi separazione degli allegati

Specifica se suddividere tutti gli allegati al messaggio di posta elettronica quando un intero messaggio di posta elettronica viene aggiunto come allegato. Il messaggio di posta elettronica e gli allegati vengono suddivisi in file separati e associati ai ticket. Applicabile solo quando è selezionata l'opzione Allega intero messaggio di posta elettronica.

Consenti anonimo

Specifica se è possibile creare i ticket da messaggi di posta anonimi.

Salva messaggi di posta elettronica sconosciuti

Specifica se salvare i messaggi di posta elettronica non elaborati dalla regole definite nella casella di posta. Questi messaggi di posta elettronica vengono archiviati in $NX_ROOT/site/mail_unknown.

Usa indirizzo per le risposte

Specifica se utilizzare l'indirizzo di posta elettronica alternativo per le risposte.

Usa crittografia TLS

Specifica se utilizzare supporto Transport Layer Security (TLS) nei messaggi di posta elettronica.

Percorso certificato dell'autorità di certificazione

Specifica il percorso in cui è stato distribuito il certificato attendibile.

Nota: Per la configurazione con disponibilità avanzata, verificare di aver distribuito il certificato attendibile nella stessa posizione per i server in background e di standby. CA SDM supporta solo il formato di codifica in Base 64 (PEM) per i certificati dell'autorità di certificazione.

4. Fare clic su Crea Nuovo nella scheda Regole per creare una regola di casella di posta.

   Viene visualizzata la pagina Crea Nuova regola casella di posta.

   Nota: Le regole applicabili a una casella di posta non possono essere associate a un'altra casella. Per riutilizzare le stesse regole per una casella di posta diversa, ricrearle per l'altra casella. È possibile anche copiare la casella di posta esistente.

   Importante: Si consiglia di impostare la casella di posta associata come non attiva prima di configurare una regola della casella di posta. Altrimenti eventuali messaggi recuperati dal server di posta nell'intervallo tra la prima e l'ultima modifica verranno elaborati utilizzando le regole attive.

5. Compilare i campi delle regole della casella di posta (a pagina 234) in base alle proprie esigenze e fare clic su Salva.

6. Selezionare la scheda Policy per definire i criteri della casella di posta per proteggere la propria organizzazione da alcuni tipi di abuso dei messaggi di posta elettronica. Compilare i campi delle policy della casella di posta (a pagina 233) in base alle proprie esigenze e fare clic su Salva.

   La casella di posta viene creata.

Se si utilizzano più caselle di posta, il componente Mail Eater (pdm_maileater_nxd) utilizza connessioni e regole di caselle di posta per leggere ed elaborare messaggi da uno o più account su uno o più server di posta elettronica. Il componente Mail Eater viene eseguito sui server seguenti, a seconda della configurazione di CA SDM:

- Convenzionale: server primario
- Disponibilità avanzata: server in background

Il componente Mail Eater elabora le caselle di posta in serie (viene elaborata una sola casella di posta per volta) e le regole in sequenza, nel modo seguente.

a. All'avvio del server primario o in background, il componente Mail Eater legge le tabelle seguenti nel database:

   usp_mailbox

   Rappresenta una connessione a un server di posta elettronica.

   usp_mailbox_rules

   Rappresenta le regole che si applicano alla connessione (usp_mailbox).

   Contact_Method

   Rappresenta i metodi di contatto utilizzati per le risposte automatiche.

   Document_Repository

   Rappresenta i repository documenti utilizzati per l'archiviazione degli allegati.

   Il componente Mail Eater rileva automaticamente eventuali modifiche apportate agli oggetti in ognuna di queste tabelle, inclusa l'aggiunta di ulteriori oggetti. Se viene apportata una modifica alla tabella a usp_mailbox o usp_mailbox_rule, l'intervallo di polling delle caselle di posta interessate viene ripianificato a un secondo dopo l'applicazione della modifica.

b. In base all'intervallo definito per ogni casella di posta, il componente Mail Eater recupera tutti i messaggi nella cartella della posta in arrivo per l'account associato ed elabora i messaggi come segue:

c. Verifica l'indirizzo di posta elettronica per eventuali violazioni di policy. Se riscontra una violazione, l'elaborazione si arresta e viene coinvolto il registro standard in base alla definizione della casella di posta.

d. Confronta il messaggio di posta elettronica con ogni regola (mailbox_rule) che appartiene a tale casella di posta.

e. Se trova una regola corrispondente, invia il messaggio API di testo per la registrazione e risponde all'utente come necessario in base all'azione specificata per la regola.

   Per i messaggi di risposta, la stringa di filtro identifica l'oggetto e utilizza l'interfaccia API testo per l'elaborazione. Al termine dell'elaborazione, la risposta viene inviata all'indirizzo Rispondi a oppure Da.

f. Dopo che il daemon Mail Eater ha trovato una regola corrispondente, non vengono controllate altre regole e viene elaborato il successivo messaggio nella cartella della posta in arrivo.

g. Se non vengono trovate regole corrispondenti, il messaggio viene scartato.

   Dopo che il daemon Mail Eater ha elaborato tutti i messaggi di una cartella di posta in arrivo, i messaggi elaborati e quelli scartati vengono eliminati dal server di posta elettronica e viene pianificato il successivo intervallo di elaborazione.

Creazione di una policy di casella di posta

È possibile creare policy applicabili a tutte le azioni, alle risposte o a entrambe. L'esecuzione di tali policy è necessaria per la consegna del messaggio di posta nella cartella di posta in arrivo.

Per creare una policy di casella di posta:

1. Nella scheda Amministrazione, selezionare Posta elettronica, Caselle di posta.

   Viene visualizzata la pagina di elenco delle caselle di posta, in cui sono elencati gli attributi.

2. Fare clic sul nome della casella di posta per la quale si intende configurare le policy.

   Viene visualizzata la pagina Dettagli casella di posta.

3. Fare clic sulla scheda Policy.

   Vengono visualizzati i dettagli della policy associati alla casella di posta.

4. Fare clic su Modifica.

   Modificare i campi.

5. Compilare i campi (a pagina 232) in modo appropriato.

6. Fare clic su Salva.

   La policy della casella di posta viene impostata e attivata immediatamente.

Indirizzo di posta elettronica/Ora

Specifica il numero massimo di messaggi per indirizzo di posta elettronica all'ora. È possibile specificare i seguenti valori:

- -1—Nessun limite (impostazione predefinita)
- 0—Posta elettronica non consentita.
- 1—Numero massimo di messaggi di posta elettronica consentito.

Violazione registro

Registra la violazione al registro standard. È possibile specificare i seguenti valori:

- Non registrare
- Solo prima violazione (impostazione predefinita)
- Tutte le violazioni

Nota: l'opzione Solo prima violazione mantiene un elenco degli indirizzi di posta elettronica associati ai messaggi che violano le policy delle caselle di posta e utilizza questo elenco per evitare che vengano registrate voci duplicate nel registro. Le voci dell'elenco vengono cancellate quando si riavvia il daemon Mail Eater. Tuttavia, se si modifica l'impostazione Solo prima violazione e si seleziona una delle altre impostazioni e viceversa, l'elenco di indirizzi di posta elettronica registrati per questa impostazione non viene cancellato. Se una casella di posta registra più violazioni durante l'uso di questa impostazione, è consigliabile riavviare il daemon Mail Eater regolarmente per cancellare le voci dell'elenco oppure usare l'opzione Non registrare.

Elenco Inclusioni

Specifica gli indirizzi di posta elettronica o i domini autorizzati a elaborare messaggi di posta elettronica; sono consentiti solo gli indirizzi di posta elettronica inclusi nell'elenco. È possibile specificare più indirizzi o domini delimitandoli con una virgola, un punto e virgola, un carattere spazio o un'interruzione di riga. L'immissione di un asterisco ('*') indica il “dominio mondiale” e ricerca tutte le corrispondenze per tutti i domini non presenti in Elenco Esclusioni.

Elenco Esclusioni

Specifica gli indirizzi di posta elettronica o i domini non autorizzati a elaborare messaggi di posta elettronica. È possibile specificare più indirizzi o domini delimitandoli con una virgola, un punto e virgola, un carattere spazio o un'interruzione di riga.

Nota: gli indirizzi in Elenco Esclusioni hanno la priorità su tutti i valori presenti in Elenco Inclusioni. Gli indirizzi in Elenco Inclusioni hanno la priorità sui domini presenti in Elenco Esclusioni e possono fornire eccezioni specifiche per mittenti specifici in un dominio normalmente vietato. I domini presenti in Elenco Esclusioni hanno la priorità sul dominio mondiale presente in Elenco inclusioni. Il dominio mondiale non può essere usato in Elenco esclusioni.

Campi delle policy della casella di posta

È possibile utilizzare i campi seguenti per implementare la policy:

Indirizzo di posta elettronica/Ora

Specifica il numero di messaggi di posta elettronica all'ora che qualsiasi indirizzo di posta elettronica è autorizzato a inviare a quella casella di posta. Se un indirizzo di posta elettronica supera tale limite, viene aggiunto all'elenco delle esclusioni e non vengono più elaborati messaggi provenienti da quell'indirizzo di posta elettronica mittente per quella casella di posta finché non si rimuove l'indirizzo dall'elenco delle esclusioni.

Violazione registro

Specifica se registrare gli indirizzi di posta elettronica che violano la policy nel file stdlog.

Elenco Inclusioni

Specifica gli indirizzi di posta elettronica (ad esempio, user@company.com) o i domini di posta elettronica (ad esempio, company.com) che sono autorizzati a inviare messaggi di posta elettronica.

L'elenco delle inclusioni predefinito di ogni casella di posta è un asterisco (*). Un asterisco da solo come nome intero in questo elenco specifica il Dominio mondo e rappresenta tutti i domini di posta elettronica non inclusi nell'elenco delle esclusioni. Questa rappresentazione risolve in questo modo l'ambiguità che potrebbe sorgere dal considerare l'elenco delle inclusioni come l'elenco completo dei domini consentiti oppure come le eccezioni ai domini specificati nell'elenco delle esclusioni:

- Un elenco delle inclusioni che include il Dominio mondo specifica che tutte le altre voci dell'elenco delle inclusioni sono eccezioni all'elenco delle esclusioni e che solo i domini o gli indirizzi nell'elenco delle esclusioni sono bloccati (ad eccezione di indirizzi specifici nell'elenco delle inclusioni).
- Un elenco delle inclusioni che non contiene il Dominio mondo specifica che sono autorizzati solo gli indirizzi e i domini elencati nell'elenco delle inclusioni e solo se il dominio del mittente (se l'indirizzo specifico non è nell'elenco delle inclusioni) o l'indirizzo del mittente non sono nell'elenco delle esclusioni.

Elenco Esclusioni

Specifica gli indirizzi di posta elettronica (ad esempio, user@company.com) o i domini di posta elettronica (ad esempio, company.com) che non sono autorizzati a inviare messaggi di posta elettronica.

Nota: Le policy della casella di posta elettronica interessano solo la casella di posta elettronica associata. Un indirizzo che viene aggiunto automaticamente a un elenco delle esclusioni di una casella di posta per violazione del numero massimo di messaggi non viene automaticamente aggiunto all'elenco delle esclusioni di altre caselle di posta, né il numero di messaggi è utilizzato per altre caselle di posta.

Campi regola casella di posta

Completare i seguenti campi della regola della casella di posta secondo le esigenze.

Sequenza

Specifica il numero di sequenza della regola. I messaggi vengono valutati in base alle regole secondo il numero di sequenza, dal più basso al più alto.

Casella di posta

Specifica la casella di posta a cui appartiene la regola.

Attivo

Imposta la regola come attiva o non attiva.

Filtro

Specifica la parte del messaggio di posta in cui eseguire la ricerca del criterio di filtro, ad esempio Oggetto contenente. Per ulteriori informazioni, consultare l'argomento Ricerca di corrispondenze di testo nelle regole della casella di posta (a pagina 239).

Stringa filtro

Specifica una stringa di espressione regolare che corrisponda al contenuto del messaggio di posta elettronica. Ad esempio, [\t\r\n]request[\t\r\n]. Il segnaposto {{object_id}} consente di specificare il valore dell'elemento che l'interfaccia API di testo utilizza per associare il messaggio a un ticket specifico. Per ulteriori informazioni, consultare gli argomenti Restrizioni dell'identificatore dell'oggetto stringa filtro (a pagina 241) e Caratteri speciali nelle espressioni regolari (a pagina 242).

Ignora maiuscole/minuscole

Specifica se utilizzare la distinzione tra maiuscole/minuscole nella ricerca.

Azione

Specifica l'azione da intraprendere in caso di corrispondenza con i criteri di filtro, ad esempio Crea/Aggiorna oggetto.

Nota: per informazioni sulle azioni della regola, consultare la *Guida all'amministrazione*.

Oggetto azione

Visualizza il tipo di oggetto del ticket a cui si applicano le azioni del messaggio, ad esempio Richiesta.

Tipo elemento minimo

Consente di impostare il tipo minimo di elemento sui seguenti valori:

NESSUNO

Non specifica nessuna validazione degli elementi. Questo valore equivale a non aggiungere la parola chiave al file di input. Accetta inoltre comandi ID ticket dell'interfaccia API testo.

PROTETTO

Convalida un ticket nei confronti dell'hash per conferma. Se la conferma non riesce, l'elemento viene considerato non valido e la posta elettronica non viene filtrata quando il filtro cerca un elemento ({{object_id}}).

PROTEZIONE

Convalida il numero di ticket da un blocco dati crittografato. Se il valore non è un numero di ticket crittografato valido, l'elemento è considerato non valido e la posta elettronica non viene filtrata quando il filtro cerca un elemento ({{object_id}}).

Nota: sono consentiti tipi che sono più sicuri del tipo impostato. In altre parole, se si imposta il tipo minimo su PROTETTO sono consentiti entrambi i tipi PROTETTO e PROTEZIONE, ma non NESSUNO. Inoltre, se è selezionato il tipo PROTETTO o PROTEZIONE, i comandi ID ticket di API di testo non vengono accettati. Per ulteriori informazioni sugli elementi, consultare l'argomento Considerazioni sull'uso degli elementi (a pagina 243).

Risposta

Specifica un metodo di notifica per l'invio di una risposta automatica. Ad esempio, Posta elettronica. Se non si imposta questa opzione, non viene restituita alcuna risposta. La risposta indica il successo o l'insuccesso delle azioni eseguite per il messaggio ed è separata da qualsiasi altra notifica. Se si utilizzano più caselle di posta, si consiglia di utilizzare il metodo di notifica per configurare le risposte ai messaggi di posta elettronica (a pagina 249).

Oggetto di risposta

Specifica un oggetto per la risposta, ad esempio Risposta di Service Desk.

Scrivi su stdlog

Se il criterio di filtro corrisponde, scrive il testo del messaggio di posta elettronica nel registro standard (stdlog).

Prefisso voce di registro

Specifica un prefisso da aggiungere alle voci del registro standard quando viene scritto il testo di un messaggio di posta elettronica. Utilizzare questa opzione per consentire la corrispondenza tra voci di registro e regole.

Aggiungi riga oggetto

Aggiunge la riga dell'oggetto del messaggio originale al corpo del messaggio prima dell'elaborazione. È possibile aggiungere, anteporre oppure non aggiungere la riga dell'oggetto. La riga dell'oggetto viene aggiunta alla descrizione del ticket oppure a un commento del registro, in base alle azioni definite per il messaggio.

Impostazioni predefinite TextAPI

Specifica ulteriori comandi predefiniti per l'API testo quando il filtro corrisponde. Si combina con il contenuto della sezione [EMAIL_DEFAULTS] del file text_api.cfg. Il campo Impostazioni predefinite TextAPI include comandi della parola chiave TextAPI applicati ad un ticket quando quest'ultimo viene creato da un messaggio di posta elettronica che corrisponde ad una regola della casella di posta. I comandi non vengono applicati quando il messaggio interessa un ticket esistente.

Per specificare i comandi del campo Impostazioni predefinite API di testo, inserire ciascun comando in una riga separata. Formattare i comandi nel modo seguente:

`OBJECT.FIELD=`*`value`*

Nota: non includere un simbolo di percentuale iniziale (%), richiesto solo per i comandi corrispondenti incorporati nel corpo del messaggio di posta elettronica.

Ad esempio, formattare i comandi nel modo seguente:

```
REQUEST.PRIORITY=3
PROBLEM.CATEGORY=Facilities
INCIDENT.GROUP=Plumbing
```

API di testo - Ignora elementi in entrata

Specifica ulteriori Ignora dettagli per l'API testo quando il filtro corrisponde. Si combina con il contenuto della sezione [EMAIL_IGNORE_INCOMING] del file text_api.cfg.

Il campo API di testo - Ignora elementi in entrata elenca i comandi della parola chiave TextAPI di cui non è consentito l'uso in un messaggio di posta elettronica in entrata. Tutti i comandi elencati in questo campo vengono ignorati quando vengono rilevati in un messaggio di posta elettronica in entrata.

Per specificare i comandi API di testo - Ignora elementi in entrata, procedere come segue:

a. Inserire ogni comando su una riga separata nel campo API di testo - Ignora elementi in entrata.

b. Formattare i comandi nel modo seguente:

   ```
   OBJECT.FIELD
   ```

   Nota: non includere un simbolo di percentuale iniziale (%), richiesto solo per i comandi corrispondenti incorporati nel corpo del messaggio di posta elettronica.

Ad esempio, formattare i comandi nel modo seguente:

```
CHANGE.ASSIGNEE
PROBLEM.GROUP
REQUEST.EFFORT
```

c. Definire tutti i comandi utilizzati nel campo della sezione [KEYWORDS] del file text_api.cfg. Il file si trova nella sottodirectory “site” della directory di installazione di CA SDM.

Dettagli

Specifica informazioni sulla regola.

Testo del messaggio di operazione completata correttamente

Specifica il contenuto in formato testo normale di un messaggio di risposta che viene inviato quando un messaggio viene elaborato correttamente. Ad esempio:

```
Grazie per aver inviato un aggiornamento della sua richiesta. Un addetto del supporto tecnico la contatterà entro 24 ore.
```

È possibile immettere anche una frase di notifica, se è già stata creata. Ad esempio, è possibile utilizzare una frase di notifica per le risposte automatiche ai messaggi di posta elettronica.

```
Grazie per aver inoltrato la richiesta.
@{notification_phrase[notification phrase code].phrase}
```

HTML di operazione completata correttamente

Specifica il contenuto in formato HTML di un messaggio di risposta che viene inviato quando un messaggio viene elaborato correttamente. Le opzioni seguenti consentono di modificare e visualizzare in anteprima il testo HTML:

Modifica HTML di operazione completata correttamente

Apre l'Editor HTML da utilizzare per la formattazione del testo HTML.

Visualizzazione rapida

Mostra in anteprima l'HTML.

Origine HTML

Mostra l'origine HTML.

È possibile utilizzare anche una frase di notifica, ad esempio,

```
Grazie per aver inoltrato la richiesta.</p>
@{notification_phrase[notification phrase code].phrase}</p>
```

Testo del messaggio di errore

Specifica il contenuto in formato testo normale di un messaggio di risposta che viene inviato quando un messaggio non viene elaborato correttamente. È possibile immettere anche una frase di notifica, se è già stata creata. Ad esempio, è possibile utilizzare il testo seguente:

```
Grazie per aver inoltrato la richiesta.
@{notification_phrase[notification phrase code].phrase}
```

HTML di errore

Specifica il contenuto in formato HTML di un messaggio di risposta che viene inviato quando un messaggio non viene elaborato correttamente.

Creazione di regole della casella di posta

È possibile creare regole che consentano di riconoscere parole chiave o elementi specifici nei messaggi in arrivo, nonché di eseguire azioni, inviare risposte (o entrambi) per tutti i messaggi in arrivo contenenti le parole chiave o gli elementi specificati.

Nota: Le regole applicabili a una casella di posta non possono essere associate a un'altra casella. Per riutilizzare le stesse regole per una casella di posta diversa, ricrearle per l'altra casella. È possibile anche copiare la casella di posta esistente.

Importante: Si consiglia di impostare la casella di posta associata come non attiva prima di configurare una regola della casella di posta. Altrimenti eventuali messaggi recuperati dal server di posta nell'intervallo tra la prima e l'ultima modifica verranno elaborati utilizzando le regole attive.

Per creare una regola della casella di posta:

1. Nella scheda Amministrazione, selezionare Posta elettronica, quindi Regole della casella di posta.

   Viene visualizzata la pagina di elenco delle regole della casella di posta.

2. Fare clic su Crea nuovo.

   Viene visualizzata la pagina dei dettagli delle regole della casella di posta.

3. Compilare i campi (a pagina 234) in modo appropriato.
4. Fare clic su Salva.

   La regola della casella di posta è stata creata ed è attiva.

Azioni delle regole della casella di posta

Le regole della casella di posta consentono di eseguire le seguenti azioni relative alla posta elettronica:

- Ignora posta elettronica—Il messaggio di posta elettronica non viene elaborato e non viene fornita alcuna risposta.

  Questa azione è utile per messaggi a livello di sistema, quali messaggi di Fuori sede o errori di recapito posta.

- Ignora messaggio di posta e Rispondi—Il messaggio di posta elettronica non viene elaborato e viene fornita una risposta al mittente. I messaggi di posta elettronica di risposta utilizzano i messaggi Risposta del messaggio di operazione riuscita e i messaggi Errore di risposta vengono ignorati.
- Aggiorna oggetto—Utilizza la stringa di filtro per stabilire l'identificatore oggetto (ad esempio, %Incident:{{object_id}}% nel messaggio) e invia una richiesta di aggiornamento all'interfaccia API testo. Se l'identificatore oggetto non viene trovato, l'interfaccia API testo non esegue alcuna azione.

  Questa azione gestisce generalmente risposte a messaggi di posta elettronica quando l'identificatore oggetto è incorporato nel messaggio di posta elettronica. Se manca un identificatore oggetto, viene generalmente inviato il messaggio di errore risposta.
- Crea/Aggiorna oggetto—Utilizza la stringa di filtro per stabilire l'identificatore oggetto (ad esempio, %Incident:{{object_id}}% nel messaggio) e invia una richiesta di aggiornamento all'interfaccia API testo. Se l'identificatore oggetto viene trovato, l'interfaccia API testo aggiorna un ticket. Se l'identificatore oggetto non viene trovato, l'interfaccia API testo crea un ticket.

  Questa azione è il comportamento standard del daemon di posta elettronica (Mail Eater) in cui il messaggio contiene o meno parole chiave dell'interfaccia API testo.

Nota: per informazioni sulla configurazione delle regole dalla casella di posta, consultare la *Guida in linea*.

Ricerca di corrispondenze di testo nelle regole della casella di posta

Le regole della casella di posta utilizzano espressioni regolari per la ricerca di corrispondenze di testo. Si considerino i seguenti spazi vuoti che si applicano alle espressioni regolari nelle regole della casella di posta:

\t

Specifica una tabulazione orizzontale.

\r

Specifica un carattere di ritorno a capo.

\n

Specifica un carattere di avanzamento riga o di nuova riga.

I caratteri che rappresentano le interruzioni di riga nel testo possono variare da un sistema operativo all'altro, da un server di posta elettronica all'altro, da un client di posta elettronica all'altro. Ad esempio:

- UNIX utilizza il carattere \n.
- Microsoft utilizza il carattere \r\n
- Macintosh utilizza il carattere \r
- MacOS X utilizza il carattere \n

In alcuni casi, gli elementi di elaborazione della posta elettronica di CA SDM scambiano o sostituiscono uno di questi caratteri di interruzione di riga con un altro carattere per stabilire o mantenere una distinzione tra vari elementi di testo, ad esempio il testo del messaggio e i parametri correlati. Pertanto, quando si desidera utilizzare un'interruzione di riga o di paragrafo, costruire i filtri in modo tale che il carattere \r corrisponda al carattere \n, a prescindere da quale dei due viene trovato. Se si desidera indicare un'interruzione di riga tra due parole chiave, costruire i filtri in modo tale che possa essere trovata una corrispondenza per una sequenza di uno o più caratteri \r e \n.

Il ritorno a capo automatico del client di posta elettronica che invia un messaggio può provocare interruzioni di riga non previste al centro del testo che dovrebbe corrispondere alla stringa di filtro quando la stringa di filtro cerca nel corpo del messaggio. Uno spazio può trasformarsi in un ritorno a capo, un avanzamento di riga o entrambi oppure un ritorno a capo, un avanzamento di riga o entrambi possono essere inseriti dopo uno spazio. Se un messaggio è composto in HTML e contiene elenchi puntati e numerati o paragrafi rientrati, dopo che il client di posta converte e invia il messaggio, nel messaggio potrebbero essere presenti delle tabulazioni. Se si includono spazi al centro di una stringa di filtro, utilizzare un blocco Espressione regolare che rappresenta qualsiasi spazio vuoto di dimensioni variabili. Questo blocco è [\t\r\n]+ (aperta parentesi, spazio, barra rovesciata, t, barra rovesciata, r, barra rovesciata, n, chiusa parentesi, segno più) e rappresenta qualsiasi sequenza di uno o più spazi, tabulazioni, ritorni a capo e avanzamenti di riga.

Esempio: utilizzo di [\t\r\n] per trovare la corrispondenza esatta di una parola chiave

L'esempio riportato di seguito dimostra come utilizzare spazi vuoti per trovare la corrispondenza esatta della parola chiave "request" e non altre possibili parole chiave quali:

```
requester
requesting
requested
orequestra
```

Per trovare solo la parola chiave "request", far precedere e seguire la parola chiave "request" da uno o più spazi vuoti, come indicato di seguito:

```
[ \t\r\n]request[ \t\r\n]
```

Il daemon Mail Eater trova solo la corrispondenza esatta della parola "request" oppure la parola come parte di una frase e non come parte di un'altra parola, ad esempio "requester".

Restrizioni dell'identificatore dell'oggetto stringa filtro

Alle stringhe filtro delle regole della casella di posta che determinano l'ID oggetto (ad esempio, %Incident:{{object_id}}%) in un messaggio di posta elettronica si applicano delle restrizioni. Il testo che circonda un ID oggetto ({{object_id}}) deve essere non ambiguo sia in termini di contenuto che di lunghezza. Il testo deve definire con chiarezza l'inizio e la fine del valore dell'elemento ID ticket che si trova nel testo.

Alla modalità con cui il daemon Mail Eater interpreta l'*inizio* del valore dell'elemento ID ticket si applicano le seguenti restrizioni:

- Il segnaposto {{object_id}} non deve essere il primo elemento della stringa di filtro. Almeno un carattere, e generalmente una parola chiave distintiva, o una sequenza di lettere, numeri e simboli devono precedere la parola chiave ID oggetto.
- Il carattere immediatamente precedente al segnaposto {{object_id}} non deve essere un carattere ripetibile o opzionale (ovvero, un carattere che ha un segno più (+), un asterisco (*) o un punto di domanda (?)) che può essere parte di un valore dell'elemento ID ticket. Caratteri ripetibili o opzionali rischiano di essere ambigui con l'inizio del valore dell'elemento ID ticket, a meno che non siano spazi vuoti. Spazi vuoti (spazio, tabulazione, ritorno a capo, avanzamento riga) non devono fare parte del valore dell'elemento ID ticket.
- Il carattere immediatamente precedente al segnaposto {{object_id}} non deve essere un insieme di caratteri racchiusi tra parentesi ripetibili o opzionali che includono caratteri che possono fare parte del valore dell'elemento ID ticket.

Alla modalità con cui il daemon Mail Eater interpreta la *lunghezza* del valore dell'elemento ID ticket si applicano le seguenti restrizioni:

- Il segnaposto {{object_id}} non deve essere l'ultimo elemento della stringa di filtro. Uno o più caratteri devono seguire il segnaposto {{object_id}}.
- Il carattere immediatamente seguente al segnaposto {{object_id}} non deve essere un carattere ripetibile o opzionale (ovvero, un carattere che ha un segno più (+), un asterisco (*) o un punto di domanda (?)) che può essere parte di un valore dell'elemento ID ticket. Caratteri ripetibili o opzionali rischiano di essere ambigui con la fine del valore dell'elemento ID ticket, a meno che non siano spazi vuoti. Spazi vuoti (spazio, tabulazione, ritorno a capo, avanzamento riga) non devono fare parte del valore dell'elemento ID ticket.

- Il primo carattere dopo il segnaposto {{object_id}} non deve essere un carattere che può fare parte del valore dell'elemento ID ticket.
- Evitare i seguenti caratteri immediatamente prima e dopo il segnaposto {{object_id}}:
  - lettere tutte maiuscole o minuscole
  - valori numerici
  - il segno più (+)
  - la barra (/)
  - la virgola (,)
  - il punto (.), perché può rappresentare qualsiasi carattere ad eccezione di un'interruzione di riga, e può pertanto essere uno qualsiasi dei caratteri di questo elenco

  poiché ognuno di questi caratteri può essere presente all'interno del valore dell'elemento ID ticket. Quando un insieme racchiuso tra parentesi (più caratteri tra parentesi che possono essere tutti trovati dal filtro) precede o segue il segnaposto {{object_id}}, l'insieme tra parentesi non deve contenere alcuno di questi caratteri.

Caratteri speciali nelle espressioni regolari

Per cercare corrispondenze di testo, i filtri delle regole della casella di posta utilizzano le regole delle espressioni regolari ASCII con caratteri speciali in stile C.

Importante: È consigliabile conoscere la sintassi Regex per utilizzare caratteri speciali nelle espressioni regolari.

Ad esempio, si considerino i seguenti caratteri speciali per schemi Regex che si applicano a espressioni regolari nelle regole della casella di posta:

\t

Specifica una tabulazione orizzontale. Nelle stringhe di filtro per le regole della casella di posta, \t corrisponde all'inizio e alla fine del testo (e tabulazioni) ed è specifico del daemon Mail Eater.

\r

Specifica un ritorno a capo (ritorno all'inizio della riga corrente).

Nota: non utilizzare \r per cercare oggetti di messaggi o indirizzi di mittenti.

\n

Specifica una nuova riga (combinazione di avanzamento riga e ritorno a capo).

Nota: non utilizzare \n per cercare oggetti di messaggi o indirizzi di mittenti.

\t, \r e \n sono i caratteri speciali che ricorrono con maggior frequenza nelle espressioni regolari per le regole della casella di posta.

Esempio: utilizzo di \t, \r e \n

`[ \t]request[ \t]`

Cerca il testo della parola "request". Le parentesi corrispondono a qualsiasi carattere dell'insieme, incluso lo spazio, pertanto [\t] corrisponde a uno spazio o a una tabulazione.

`[\r\n]+critical[ \t\r\n]`

Cerca il testo della parola "critical" all'inizio di una riga, all'inizio del messaggio e come intero contenuto di una riga. Le parentesi corrispondono a qualsiasi carattere dell'insieme e il segno + (più) corrisponde a uno o più caratteri precedenti, pertanto [\r\n]+ corrisponde e uno o più ritorni a capo e nuove righe.

Testo di esempio per frasi di notifica in una regola di casella di posta

Questo esempio contiene un testo campione da utilizzare per includere frasi di notifica in una regola di casella di posta. Quando una frase di notifica contiene interruzioni di riga o altra formattazione, è necessario definirne versioni diverse per il formato di solo testo e quello HTML.

Nella scheda Risposta del messaggio di operazione completata correttamente della pagina Aggiorna regola casella di posta, utilizzare il seguente testo nei campi Testo del messaggio di operazione completata correttamente, HTML di operazione completata correttamente o in entrambi:

- Testo del messaggio di operazione completata correttamente

```
Grazie per aver inoltrato la richiesta.
@{notification_phrase[IncidentURL1].phrase}
```

- HTML di operazione completata correttamente

```
Grazie per aver inoltrato la richiesta.</p>
@{notification_phrase[IncidentURL1H].phrase}</p>
```

Nota: Per ulteriori informazioni sulle frasi di notifica definite nella scheda Amministrazione, Notifiche, Frasi di notifica, consultare la *Guida in linea*.

Ulteriori informazioni:

Frasi e codici di notifica (a pagina 218)
Sintassi delle frasi di notifica (a pagina 220)

Considerazioni sull'uso degli elementi

Per *elemento* di posta elettronica si intende un artefatto generato dal processo di posta elettronica, ad esempio un indirizzo di posta elettronica che viene incluso in un messaggio di posta elettronica inoltrato. L'interfaccia API testo utilizza gli elementi che contengono un ID ticket (ad esempio, un numero di riferimento) per le risposte. Quando viene trovato un ID ticket, viene impostata una parola chiave esistente dell'interfaccia API testo (ad esempio, %INCIDENT_ID) e aggiunta all'input per l'interfaccia API testo. Il daemon Mail Eater identifica che una risposta è associata a un determinato ticket trovando l'elemento nel messaggio.

Le regole della casella di posta consentono di specificare l'elemento e il valore utilizzato da API di testo. Ad esempio, è possibile definire una regola per Incidenti, quale Incident:{{object_id}}%. Quando la regola trova Incident:1234, l'interfaccia API testo usa %INCIDENT_ID=1234 (1234 è il ref_num dell'incidente). Poiché l'elemento deve essere univoco nel messaggio di posta elettronica e facile da trovare, è possibile renderlo più distintivo, ad esempio %Incident:{{object_id}}%. Un eventuale segno di percentuale (%), spazio o altro carattere che non può apparire nel valore dell'elemento deve essere apposto a {{object_id}}. Possono fare parte del valore lettere maiuscole e minuscole, numeri, barre, virgole e segni più. Gli elementi protetti sono codificati con codifica Base64 dopo la crittografia. Se non si utilizzano elementi protetti, gli eventuali caratteri che seguono l'elemento non devono essere contenuti nel suffisso dell'ID ticket, che è stato configurato per tale tipo di ticket.

Quando si usa la stringa di filtro delle regole della casella di posta per identificare l'elemento ID ticket, la parola chiave {{object_id}} rappresenta la posizione nella stringa di filtro dove è previsto l'elemento ID ticket. La parola chiave distingue tra maiuscole e minuscole, anche se la regola della casella di posta non fa questa distinzione.

Esempio: uso di elementi nella posta elettronica

Di seguito è riportato un esempio di formato ARTIFACT da utilizzare in una regola di casella di posta per un ticket richiesta di cambiamento.

Utilizzo: %REQUEST=@{call_req_id.ref_num}%

Esempio: %REQUEST=1234%

Quando si costruisce la stringa di filtro di una regola della casella di posta, considerare quanto segue:

- Deve esistere una delimitazione netta tra l'elemento ID ticket ID e la parola chiave che lo precede e lo segue. Si consiglia vivamente di includere spazi in questo testo di delimitazione.

- Non terminare la parte della stringa di filtro che precede la parola chiave {{object_id}} con uno schema ripetibile o facoltativo corrispondente all'inizio dell'elemento ID ticket e non terminare con uno schema la cui lunghezza è ambigua. Ad esempio, la stringa di filtro non deve contenere request(er|ed|ing)?{{object_id}}, poiché questa costruzione provoca un'ambiguità relativa alla desinenza er, ed o ing che potrebbe essere la fine del testo oppure parte del prefisso di un ID ticket non protetto.
- La parte della stringa di filtro che segue la parola chiave {{object_id}} non deve iniziare secondo uno schema ripetibile o facoltativo che potrebbe corrispondere alla fine dell'elemento ID ticket, non deve iniziare con uno schema la cui lunghezza è ambigua e deve contenere almeno un elemento spazio. Ad esempio:
  - La stringa di filtro non deve contenere {{object_id}}[A-Z]?, poiché [A-Z]? potrebbe corrispondere all'ultimo carattere dell'elemento ID ticket.
  - La stringa di filtro non deve terminare con {{object_id}}Item, in quanto Item potrebbe essere visualizzato nell'elemento ID ticket, sia come suffisso di un ID ticket in un elemento di formato testo normale o di formato PROTECTED sia come caratteri in un elemento di formato SECURE.
  - {{object_id}} Item è invece accettabile poiché lo spazio non può fare parte di un elemento ID ticket e non fa parte di un elemento ID ticket di solo testo o di formato PROTECTED. Tuttavia, {{object_id}}[\t\r\n]+Item (aperta parentesi, spazio, barra rovesciata, t, barra rovesciata, r, barra rovesciata, n, chiusa parentesi, segno più, Item) è una costruzione migliore, poiché [\t\r\n]+ compensa l'ambiguità inserendo un'interruzione di riga dopo {{object_id}}.
- Quando si costruiscono stringhe di filtro per altre regole della casella di posta, evitare di utilizzare una stringa di filtro che include completamente un'altra stringa di filtro di regola della casella di posta o in cui la parte che precede o succede la parola chiave {{object_id}} include completamente tale parte di un'altra stringa di filtro di regola della casella di posta. In base all'ordine con cui vengono verificati questi filtri, una corrispondenza di messaggio pensata per un filtro può corrispondere a un'altra, con una parte dell'elemento ID ticket che corrisponde al testo aggiuntivo che distingue tra le due stringhe di filtro.

Guida all'amministrazione - Come creare una regola della casella di posta che corrisponde a ogni messaggio in entrata

Questo nuovo argomento riguarda la *Guida all'amministrazione* nel capitolo "Implementazione dei criteri" nella sezione Amministrazione della posta elettronica, Regole della casella di posta.

È possibile creare una regola della casella di posta che corrisponda ad ogni messaggio in entrata non filtrato da un'altra regola.

Per creare questo tipo di regola, impostare il filtro come Oggetto contenente e la stringa filtro come un punto e un asterisco (".*").

- Un punto corrisponde ad ogni carattere ad eccezione dell'interruzione di riga.
- Un asterisco corrisponde a zero o più occorrenze del simbolo immediatamente precedente.

Di conseguenza, questa combinazione corrisponde a zero o più caratteri che non sono interruzioni di riga.

Esempio: una regola della casella di posta "Catch-All"

Questo esempio mostra come utilizzare una combinazione ".*" corrispondente a ciascun messaggio in entrata:

```
Filtro = "Oggetto contenente"
Stringa filtro = ".*"
```

Utilizzo delle impostazioni predefinite dell'API di testo delle regole della casella di posta e le impostazioni API di testo - Ignora elementi in entrata

I campi Impostazioni predefinite TextAPI e API di testo - Ignora elementi in entrata consentono di specificare valori predefiniti per le regole della casella di posta in entrata e di specificare comandi di API di testo da non accettare nei messaggi di posta elettronica in entrata. Questi campi funzionano con i valori predefiniti impostati nella sezione [EMAIL_DEFAULTS] e con l'elenco di comandi proibiti nella sezione [EMAIL_IGNORE_INCOMING] del file text_api.cfg. Quando si verifica un conflitto tra la definizione presente in una regola della casella di posta e la definizione nel file text_api.cfg, si applica il valore impostato nella regola della casella di posta.

Il campo Impostazioni predefinite TextAPI include comandi della parola chiave TextAPI applicati ad un ticket quando quest'ultimo viene creato da un messaggio di posta elettronica che corrisponde ad una regola della casella di posta. I comandi non vengono applicati quando il messaggio interessa un ticket esistente.

Per specificare i comandi di Impostazioni predefinite di TextAPI, procedere come segue:

1. Inserire ogni comando su una riga separata nel campo API di testo - Ignora elementi in entrata.
2. Formattare i comandi nel modo seguente:

   OBJECT.FIELD=*value*

   Nota: non includere un simbolo di percentuale iniziale (%), richiesto solo per i comandi corrispondenti incorporati nel corpo del messaggio di posta elettronica.

   Ad esempio, formattare i comandi nel modo seguente:

   ```
   REQUEST.PRIORITY=3
   PROBLEM.CATEGORY=Facilities
   INCIDENT.GROUP=Plumbing
   ```

Il campo API di testo - Ignora elementi in entrata elenca i comandi della parola chiave TextAPI di cui non è consentito l'uso in un messaggio di posta elettronica in entrata. Tutti i comandi elencati in questo campo vengono ignorati quando vengono rilevati in un messaggio di posta elettronica in entrata.

Per specificare i comandi API di testo - Ignora elementi in entrata, procedere come segue:

1. Inserire ogni comando su una riga separata nel campo API di testo - Ignora elementi in entrata.
2. Formattare i comandi nel modo seguente:

   ```
   OBJECT.FIELD
   ```

   Nota: non includere un simbolo di percentuale iniziale (%), richiesto solo per i comandi corrispondenti incorporati nel corpo del messaggio di posta elettronica.

   Ad esempio, formattare i comandi nel modo seguente:

   ```
   CHANGE.ASSIGNEE
   PROBLEM.GROUP
   REQUEST.EFFORT
   ```

3. Definire tutti i comandi utilizzati nel campo della sezione [KEYWORDS] del file text_api.cfg. Il file si trova nella sottodirectory "site" della directory di installazione di CA SDM.

Modalità di configurazione delle risposte tramite posta elettronica

Le notifiche di posta elettronica utilizzate nelle caselle di posta sono specifiche delle risposte inviate a un contatto in risposta ai suoi messaggi di posta elettronica. Ad esempio, è possibile configurare la posta elettronica in modo tale che, quando un contatto fa clic sul collegamento di risposta in una notifica di posta elettronica, il messaggio di risposta sia indirizzato a una casella di posta.

Nota: questa impostazione è diversa dalle normali notifiche di posta elettronica.

Procedere come descritto di seguito:

1. Aprire l'interfaccia utente Web di CA SDM (a pagina 191).
2. Verificare di avere configurato la casella di posta per la posta elettronica in entrata (a pagina 213).
3. Configurare il server di posta elettronica. (a pagina 248)
4. (Facoltativo) Specificare un indirizzo per le notifiche di posta elettronica nella definizione del contatto.

   Nota: Selezionare Gestione protezione e ruoli, Contatti nella scheda Amministrazione e selezionare il contatto da modificare.

5. Modificare il metodo di notifica della posta elettronica (a pagina 249).

Apertura dell'interfaccia utente Web di CA SDM

Accedere all'interfaccia utente Web dai server seguenti, in base alla configurazione di CA SDM:

- Convenzionale: server primario o secondario
- Disponibilità avanzata: server applicazioni o in background

Configurazione del server di posta elettronica

Le notifiche di un evento (automatiche e manuali) vengono inviate utilizzando la definizione di un unico server di posta elettronica.

Procedere come descritto di seguito:

1. Selezionare Gestione opzioni, Posta elettronica nella scheda Amministrazione.

   Viene visualizzata la pagina Elenco Opzioni.

2. Fare clic sull'opzione di posta elettronica (a pagina 248) che si desidera installare.

   Viene visualizzata la pagina Dettagli Opzioni.

3. Fare clic su Modifica, compilare i campi in modo appropriato e fare clic su Installa.

   Il server di posta elettronica è configurato per inviare le notifiche (messaggi di posta elettronica in uscita).

4. Ripetere la procedura finché tutte le opzioni pertinenti di Elenco Opzioni non sono state configurate.

Opzioni di posta elettronica

L'interfaccia di posta elettronica invia le notifiche tramite posta elettronica e consente la creazione di ticket da un messaggio di posta elettronica.

mail_from_address

Specifica la notifica di posta elettronica da: indirizzo. Il formato dell'indirizzo è nome visualizzato<user@company.com>.

mail_login_password

Specifica la password del server remoto SMTP.

mail_login_userid

Specifica la password del server remoto SMTP.

mail_max_threads

Specifica il numero massimo di connessioni SMTP simultanee che è possibile tentare per comunicare con il server.

mail_reply_to_address

Consente di definire l'indirizzo a cui rispondere utilizzato per le notifiche tramite posta elettronica. Questa opzione è utile nel caso in cui i messaggi di posta elettronica vengono inviati da un account utente ma si desidera che le risposte vengano inviate a un altro indirizzo di posta elettronica. Il valore predefinito corrisponde all'indirizzo di provenienza.

mail_smtp_domain_name

Definisce il nome di dominio del server SMTP. È possibile cancellare il nome di dominio impostando il valore su NESSUNO.

mail_smtp_hosts

Specifica un elenco separato da spazi di nomi host del server SMTP per le notifiche di posta elettronica.

mail_smtp_host_port

Specifica una porta SMTP per sovrascrivere la porta SMTP predefinita.

mail_smtp_security_level

Specifica il livello di protezione SMTP. Le impostazioni valide sono: 0=no protezione, 1=autenticazione base, 2=NTLM, 3=MD5 e 4=LOGIN. Se si sceglie 1, impostare le opzioni mail_login_password e mail_login_userid. La maggior parte dei server SMTP non richiede autenticazione.

mail_smtp_use_tls

Specifica l'utilizzo di TLS (Transport Layer Security) nella posta elettronica. Le impostazioni valide sono Sì=Usa crittografia TLS, No=Non usare crittografia TLS.

mail_ca_cert_path

Specifica il percorso in cui è stato distribuito il certificato attendibile.

Nota: per la configurazione con disponibilità avanzata, è necessario distribuire il certificato attendibile nella stessa posizione in tutti i server di CA SDM. CA SDM supporta solo il formato di codifica in Base 64 (PEM) per i certificati dell'autorità di certificazione.

Modifica del metodo di notifica della posta elettronica

Modificare il metodo di notifica della posta elettronica per configurare le risposte di posta elettronica.

Procedere come descritto di seguito:

1. Selezionare Notifiche, Metodi di notifica, Posta elettronica nella scheda Amministrazione e fare clic su Modifica.
2. Sulla pagina Email Update Notification Method (Metodo di notifica aggiornamento con messaggio di posta elettronica), selezionare la casella di controllo Supporto SMTP per abilitare SMTP.
3. Immettere **pdm_mail [–F from_email_address] [–T reply_to_email_address]** come metodo di notifica.

   indirizzo_da

   Specifica l'indirizzo utilizzato come indirizzo Da del messaggio. Questo indirizzo prevale sull'indirizzo del mittente indicato nella configurazione del server della posta elettronica in uscita.

   indirizzo_rispondi_a

   Specifica l'indirizzo a cui vengono inviate le risposte. Questo indirizzo prevale sull'indirizzo di risposta indicato nella configurazione del server della posta elettronica in uscita.

   Quando nella configurazione del server della posta elettronica in uscita è impostato un indirizzo di risposta, mentre nel Metodo di notifica non viene specificato alcun indirizzo di risposta, nel Metodo di notifica viene utilizzato l'indirizzo di risposta specificato nella configurazione del server della posta elettronica in uscita.

   Nota: Se si specifica la parola chiave $(REPLY_FROM) come uno dei due indirizzi, tale indirizzo viene costruito dal nome utente e dal nome host del server di posta elettronica della casella di posta. Questa parola chiave è valida solo se una regola della casella di posta utilizza il Metodo di notifica; i Metodi di notifica che la utilizzano non devono essere utilizzati ad altri scopi. Ad esempio, nome utente=dev, nome server=mail32.ca.com, $(REPLY_FROM)=dev@mail32.ca.com. Utilizzare questa parola chiave solo se il server di posta è configurato per accettare il nome del server di posta come equivalente del nome di dominio di posta. Utilizzare questa parola chiave con cautela: se il nome host non è esteso all'intero dominio nella configurazione della casella di posta (ad esempio, serverposta1 anziché server posta1.cliente7.com), non viene esteso automaticamente dall'interprete dei campi.

   Nota: gli indirizzi indirizzo_da e indirizzo_rispondi_a sono gli indirizzi che compaiono nelle intestazioni Da e Rispondi a del messaggio quando l'utente lo legge. Se gli indirizzi sono identici, è possibile specificare solo l'indirizzo_da.

4. Fare clic su Salva.

   Il metodo di notifica della posta elettronica viene modificato. Quando il contatto risponde alla notifica di posta elettronica, la risposta viene indirizzata per impostazione predefinita alla casella di posta specificata.

Ulteriori informazioni:

Utilità pdm_mail - Invio di informazioni di posta elettronica (a pagina 1176)

Identificativo di indirizzo del mittente alternativo

È possibile utilizzare un parametro -m nell'oggetto del messaggio in modo che CA SDM identifichi il mittente del messaggio utilizzando un indirizzo di posta elettronica diverso da quello da cui è stato originariamente inviato. La parola chiave -m, seguita da uno spazio e dall'indirizzo di posta elettronica riconosciuto da CA SDM, devono essere gli ultimi elementi della riga dell'oggetto. Si considerino le seguenti informazioni quando si utilizza il parametro -m nell'oggetto:

- Sia l'indirizzo Da che l'indirizzo alternativo specificato con il parametro -m vengono verificati negli elenchi delle inclusioni e delle esclusioni.
- L'indirizzo di posta elettronica specificato come indirizzo alternativo deve contenere solo l'indirizzo e non il corrispondente nome visualizzato.
- Se il parametro -m è seguito da più parole nell'oggetto, l'indirizzo alternativo non viene riconosciuto.

Polling della casella di posta

Se si verifica un errore sul server di posta elettronica in uscita, le notifiche di posta elettronica non vengono inviate e vengono accodate nella directory %NX_ROOT%\site\mail_queue. Quando il server di posta elettronica diventa nuovamente attivo, trascorso un intervallo di tempo, elabora e invia i messaggi di posta elettronica rimasti in coda. È possibile modificare l'intervallo di tempo che il sistema attende prima di riprocessare i messaggi di posta elettronica accodati quando il server di posta elettronica era occupato.

I messaggi di notifica che il server di posta elettronica in uscita non invia vengono reinviati, a meno che non venga eseguita una delle seguenti operazioni:

- Viene arrestato il componente Mail Daemon (pdm_mail_nxd) che gestisce le notifiche di posta elettronica in uscita.
- Vengono eliminati manualmente i messaggi dalla directory %NX_ROOT%\site\mail_queue.

Impostazione della variabile dell'intervallo tentativi per la posta elettronica

È possibile definire l'intervallo di tempo (in secondi) tra i tentativi non riusciti di invio di messaggi di posta elettronica dal server di posta elettronica.

Nota: CA SDM non effettua tentativi di invio di messaggi che sono stati accettati dal server di posta elettronica in uscita ma che non sono stati recapitati. Per questi messaggi sono attive le funzionalità e le policy di ripetizione dei tentativi di invio posta elettronica del server di posta elettronica in uscita.

I tentativi sono per messaggio. Se il server di posta elettronica non è disponibile per un periodo, anziché inviare tutti i messaggi contemporaneamente, viene effettuato un tentativo di invio per ogni messaggio allo scadere del relativo intervallo. Tuttavia, se si riavvia il daemon della posta elettronica in uscita, il sistema tenta di inviare contemporaneamente tutti i messaggi non inviati, e se l'invio non riesce, vengono reimpostati contemporaneamente tutti gli intervalli tra tentativi per tutti i messaggi.

L'impostazione (NX_EMAIL_RETRY_INTERVAL) del file NX.env file controlla l'intervallo tra tentativi. È possibile modificare l'impostazione predefinita dell'intervallo tra tentativi su uno o più server.

Procedere come descritto di seguito:

1. Accedere al server seguente, a seconda della configurazione di CA SDM:
   - Convenzionale: server primario
   - Disponibilità avanzata: server in background.
2. Accesso alla directory $NX_ROOT
3. Aprire il file NX.env con un editor di testo, quale WordPad.
4. Modificare il valore dell'intervallo NX_EMAIL_RETRY_INTERVAL come indicato di seguito:

   ```
   NX_EMAIL_RETRY_INTERVAL=numero_di_secondi
   ```

   NX_EMAIL_RETRY_INTERVAL

   Definisce l'intervallo di tempo (in secondi) tra i tentativi non riusciti di invio di messaggi di posta elettronica.

   numero_di_secondi

   Specifica il numero di secondi per ogni intervallo tra tentativi. Il valore predefinito è 600 secondi (10 minuti). Il valore minimo consentito è 20 secondi. Se si imposta un valore inferiore a quello minimo di 20 secondi o superiore a quello massimo di 2000000 secondi, viene utilizzato il valore predefinito di 10 minuti.
5. Salvare e chiudere il file.
6. Riavviare i server di CA SDM. Per ulteriori informazioni su come avviare il server di CA SDM, a seconda della configurazione di CA SDM, consultare lo scenario *Riavvio dei server di CA SDM* o consultare le informazioni nella *Guida per l'amministratore*.

   Le modifiche diventano effettive.

SLA (Service Level Agreement)

Uno SLA o un tipo di servizio è un accordo tra un service desk e i relativi clienti e solitamente descrive il livello di servizio fornito dal service desk. Se questo livello di servizio non viene fornito, il service desk può essere penalizzato. Ad esempio, un service desk che opera su base “pagamento per servizio” potrebbe non essere pagato se il cliente ritiene che il livello del servizio non è soddisfacente. Quindi, la maggior parte dei service desk prende sul serio gli SLA e si impegna al massimo per raggiungere il livello di servizio specificato nell'accordo.

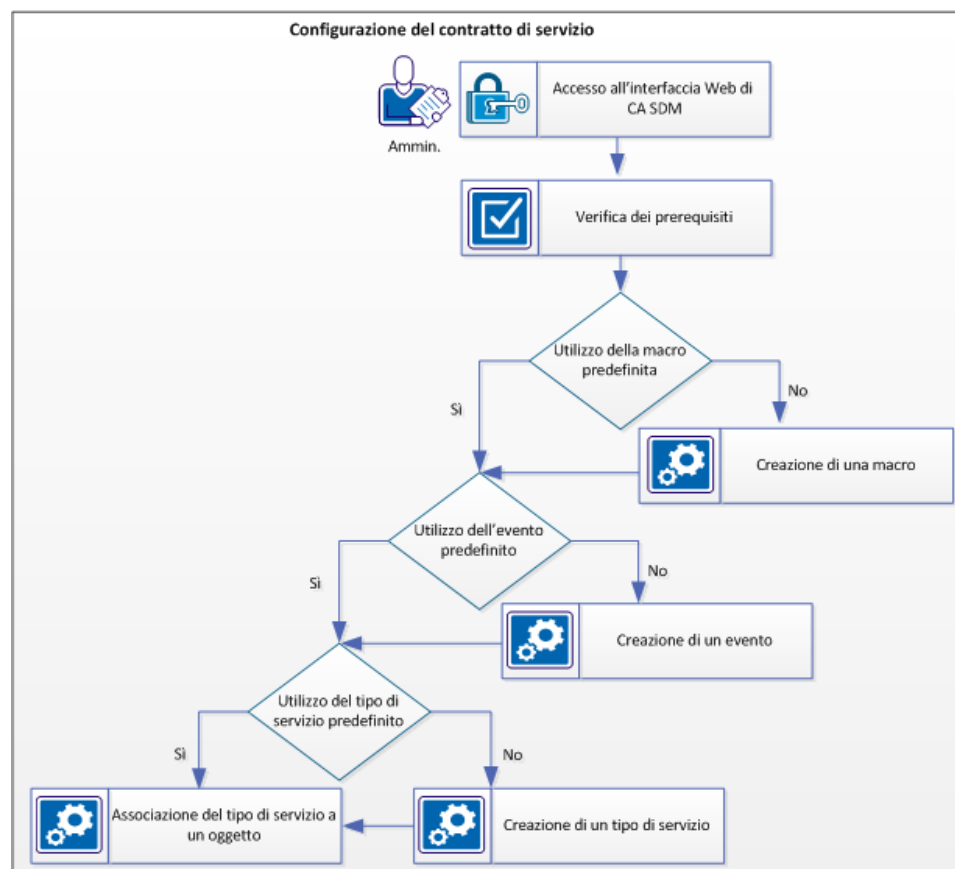
Inoltre, la maggior parte dei service desk documenta meticolosamente quando gli SLA vengono rispettati o violati. I tipi di servizio definiti con CA SDM sono realizzati per aiutare il personale del service desk a soddisfare gli SLA mantenendo inoltre i record necessari a verificare l'effettiva esecuzione degli SLA.

Modalità di configurazione dei contratti di servizio (SLA)

In CA SDM, lo SLA o il tipo di servizio descrive il livello del servizio che l'analista di service desk fornisce al cliente. Per tenere traccia degli impegni e delle pianificazioni aziendali (poiché fanno riferimento a ticket specifici), gli eventi vengono associati ai tipi di servizio. Gli eventi vengono utilizzati per definire la condizione in base alla quale il tipo di servizio viene violato e le azioni da intraprendere dopo tale violazione. Ogni evento presenta tre caratteristiche generali di comportamento, ovvero le condizioni, le azioni in caso di valore True e le azioni in caso di valore False.

- La condizione identifica lo stato misurabile di un ticket.
- L'azione identifica i processi eseguiti automaticamente nel caso in cui la condizione sia True o False dopo un determinato periodo di tempo.

Esempio: In qualità di amministratori di sistema, si desidera configurare uno SLA di 24 ore per una richiesta di hardware. Se la richiesta non viene soddisfatta, una notifica di posta elettronica viene inviata al manager del Servizio clienti e all'analista. Questo esempio viene utilizzato nello scenario per spiegare la modalità di configurazione della notifica di posta elettronica per uno SLA.

Il diagramma seguente mostra come configurare il periodo di 24 ore. Lo SLA che invia una notifica di posta elettronica, in caso di violazione:

Procedere come descritto di seguito:

1. Aprire l'interfaccia utente Web di CA SDM (a pagina 191).
2. Verificare i prerequisiti (a pagina 255).
3. Se non si desidera utilizzare una macro predefinita, creare una macro (a pagina 260).
4. Se non si desidera utilizzare un evento predefinito, creare un evento (a pagina 262).
5. Se non si desidera utilizzare un tipo di servizio predefinito, creare un tipo di servizio (a pagina 265).
6. Associare il tipo di servizio a un oggetto (a pagina 267).

Apertura dell'interfaccia utente Web di CA SDM

Accedere all'interfaccia utente Web dai server seguenti, in base alla configurazione di CA SDM:

- Convenzionale: server primario o secondario
- Disponibilità avanzata: server applicazioni o in background

Verifica dei prerequisiti

Prima di configurare lo SLA, assicurarsi di avere completato i passaggi seguenti:

- Le opzioni SLA (a pagina 255) necessarie per le esigenze dell'organizzazione sono state installate.
- Il metodo di notifica per il destinatario è stato verificato. (a pagina 192)
- Si è creato un modello di messaggio (a pagina 194) per inviare una notifica di posta elettronica in caso di violazione di uno SLA senza utilizzare un messaggio predefinito.

Opzioni SLA

Installare le opzioni SLA necessarie per l'impostazione dello SLA in base alle esigenze della propria organizzazione.

Ad esempio, nell'elaborazione SLA classica (attivata se l'opzione classic_sla_processing è installata in Gestione opzioni) è possibile applicare un solo tipo di servizio al ticket. Quando agli attributi di un ticket sono associati tipi di servizio differenti, viene utilizzato il tipo di servizio più in alto nella classificazione. La classificazione di un tipo di servizio viene definita al momento della creazione del tipo di servizio e procede in ordine crescente, ovvero il tipo di servizio più in alto nella classificazione è il numero 1, il successivo è il numero 2 e così via. Ad esempio, si supponga che alla Issue il cui tipo di servizio richiede una risoluzione in 12 ore (classificazione 2), venga assegnato un codice di priorità 1, per il quale è prevista una risoluzione di 4 ore (classificazione 1). Il tipo di servizio più in alto nella classificazione determina il comportamento del servizio per la Issue associata. In questo esempio la risoluzione in quattro ore è classificata più in alto rispetto alla risoluzione in 12- ore, quindi alla Issue viene applicato il tipo di servizio per cui è richiesta la risoluzione in 4 ore.

Da Gestione opzioni, è possibile installare le opzioni seguenti:

Nota: Per ulteriori informazioni sull'installazione o la disinstallazione delle opzioni, consultare la *Guida in linea*.

Opzione	**Descrizione**
change_allow_sla_downgrade	Modifica le proprietà dell'opzione chg_sla consentendo al sistema di abilitare automaticamente il downgrade di un tipo di servizio dell'Ordine di cambiamento. L'opzione chg_sla consente di selezionare il migliore tipo di servizio tra i vari attributi dell'Ordine di cambiamento, sebbene il tipo di servizio corrente non verrà mai sostituito con un tipo posto più in basso in classifica. Se si installa questa opzione, i tipi di servizio per tutti gli attributi interessati vengono valutati ogniqualvolta un attributo viene modificato. Il tipo di servizio dell'Ordine di cambiamento viene posizionato nella posizione più alta della classifica,anche se il nuovo tipo di servizio occupa una posizione in classifica inferiore rispetto al tipo di servizio corrente. Il tipo di servizio con il più basso valore di classificazione viene considerato il migliore. Se tutti i tipi di servizio esaminati presentano lo stesso valore di classificazione (compresi i tipi di servizio con il campo dei valori vuoto), viene selezionato il primo tipo di servizio creato nel database. È necessario installare l'opzione chg_sla affinché possa funzionare correttamente. È possibile installare un'opzione simile per il problema e la richiesta.

ttv_enabled	Consente di eseguire il daemon Ora violazione, che permette di monitorare gli SLA in tutti i ticket e le attività aperti. Questo processo non imposta la violazione SLA, bensì registra la data in cui il ticket o l'attività è stata violata nello stato corrente. Questa previsione viene aggiornata quando si aggiorna il ticket o l'attività. Questa opzione deve essere installata affinché le altre opzioni di Ora violazione funzionino correttamente. **Importante.** Questa opzione non richiede l'installazione dell'opzione classic_sla_processing.
set_sla_evt_open_date	Utilizza la data e l'orario di apertura di un Ordine di cambiamento, di una Issue o di una Richiesta come data e orario di inizio degli eventi associati. Gli eventi associati verranno avviati non appena si salva il ticket.

Verifica del metodo di notifica per il destinatario

Assicurarsi che il contatto a cui si desidera inviare la notifica sia assegnato a quel particolare metodo di notifica.

Procedere come descritto di seguito:

1. Selezionare Gestione protezione e ruoli, Contatti nella scheda Amministrazione.

   Viene visualizzata la pagina Ricerca contatto.

2. Cercare il contatto utilizzando il filtro e, tra i risultati della ricerca, selezionare il contatto a cui si desidera inviare la notifica.

   Viene visualizzata la pagina dei dettagli del contatto.

3. Selezionare Notifica nella scheda Dettagli di contatto.
4. Verificare il metodo di notifica. In base alla priorità di notifica, scegliere l'opzione richiesta. Ad esempio, si desidera inviare una notifica di posta elettronica per ogni notifica di emergenza. Selezionare l'opzione Posta Elettronica nel campo Emergenza.
5. Per modificare il metodo di notifica, fare clic su Modifica, modificare l'opzione, quindi fare clic su Salva.

   Il metodo di notifica per il contatto viene verificato.

Creazione di un modello di messaggio

Creare un modello di messaggio che contenga i valori da utilizzare per il messaggio di notifica. Quando si inviano più messaggi di notifica, è possibile usare i modelli messaggio per semplificare il carico di lavoro.

Nota: in caso di installazione dell'opzione multi-tenancy, selezionare il titolare appropriato dall'elenco a discesa. L'opzione pubblica (condivisa) consente di creare l'oggetto per tutti i titolari.

Procedere come descritto di seguito:

1. Selezionare Notifiche, Modelli messaggio dalla scheda Amministrazione.

   Viene visualizzata la pagina Elenco Modelli messaggio.

2. Fare clic su Crea Nuovo.

   Viene visualizzata la pagina Crea Nuovo modello di messaggio.

3. Compilare i campi in modo appropriato.

   Simbolo

   Definisce un identificatore univoco per questo modello di messaggio.

   Tipo di oggetto

   Specifica il tipo di oggetto associato a questo modello. Ad esempio, selezionare Richiesta/ Incidente/ Problema per qualsiasi notifica collegata a un ticket.

   Stato record

   Specifica se lo stato del modello è attivo o inattivo. Impostare lo stato su Attivo per utilizzare il modello di messaggio.

   Notifica automatica

   Specifica di inviare la notifica associata al modello automaticamente, quando l'attività viene eseguita. Ad esempio, l'utente ha impostato una notifica iniziale, l'oggetto da notificare e il modello del messaggio, ma non desidera ancora attivare le notifiche. In questo caso l'utente non seleziona Notifica automatica. Quando l'utente desidera avviare le notifiche automatiche, seleziona la casella di controllo corrispondente. La notifica viene attivata ed eseguita come definito.

   Livello notifica

   Specifica l'importanza relativa dell'invio di questa notifica. Ad esempio, selezionare Emergenza se si desidera inviare la notifica di posta elettronica al contatto non appena l'attività associata si verifica.

   Titolo messaggio di notifica

   Specifica il titolo del messaggio. È possibile utilizzare variabili per inserire il numero dell'incidente nel titolo del messaggio. Ad esempio, @{call_req_id.type.sym} @{call_req_id.ref_num} @{type.sym}.

Testo del messaggio di notifica

Specifica il contenuto del messaggio. È possibile utilizzare variabili per inserire il nome dell'analista, il nome dell'utente finale e la descrizione nel messaggio. Ad esempio:

```
@{call_req_id.type.sym} @{call_req_id.ref_num} @{type.sym}.

Assegnato a: @{call_req_id.assignee.combo_name}

Cliente: @{call_req_id.customer.combo_name}

Descrizione: @{call_req_id.description}


Fare clic sull'URL seguente per visualizzare:

@{call_req_id.web_url}
```

È possibile utilizzare la parola chiave ARTIFACT per specificare come vengono gestiti gli elementi nei messaggi in uscita, nei modelli di messaggio, nelle notifiche e nelle risposte automatiche. La parola chiave ARTIFACT utilizza i seguenti valori:

- **NONE**—Specifica nessuna convalida degli elementi. Questo valore equivale a non utilizzare alcun valore.
- **PROTECTED**—Convalida un ticket nei confronti dell'hash per conferma. Se la conferma non riesce, l'elemento è considerato non valido e il filtro non riesce quando si filtra alla ricerca di un elemento ({{object_id}}).
- **SECURE**—Esegue la decrittografia del numero ticket. Se il valore non è una password valida, l'elemento è considerato non valido e il filtro non riesce quando si filtra alla ricerca di un elemento ({{object_id}}).

Messaggio HTML

Specifica il messaggio HTML che vedrà il destinatario. Se il destinatario riceve il messaggio su un dispositivo esterno, come un telefono cellulare o PDA, il messaggio viene visualizzato soltanto in formato di testo semplice. Fare clic su Edit HTML Message (Modifica messaggio HTML) per aprire l'Editor HTML.

Visualizzazione rapida

Mostra il messaggio così come viene visualizzato dal destinatario.

Origine HTML

Mostra il messaggio nel codice di origine HTML.

4. Fare clic su Salva.

Il modello del messaggio viene creato.

Creazione di una macro di notifica di posta elettronica

È possibile creare una macro, che può essere utilizzata per aggiungere azioni agli oggetti o per verificare determinate caratteristiche o condizioni.

Nota: in caso di installazione dell'opzione multi-tenancy, selezionare il titolare appropriato dall'elenco a discesa. L'opzione pubblica (condivisa) consente di creare l'oggetto per tutti i titolari.

Procedere come descritto di seguito:

1. Selezionare Eventi e macro, Macro nella scheda Amministrazione.

   Viene visualizzata la pagina Elenco Macro.

2. Fare clic su Crea Nuovo.

   Viene visualizzata la pagina Crea nuova macro.

3. Completare i campi nel modo seguente:

   Simbolo

   Immettere un ID descrittivo per la macro.

   Tipo macro

   Selezionare il tipo per la macro. Il tipo di macro selezionato controlla i dati rimanenti che è necessario fornire.

   Nota: È possibile selezionare Esegui azione CA IT PAM solo se il flusso di lavoro CA IT PAM è configurato in CA SDM. È possibile selezionare Esegui azione CA Workflow solo se CA Workflow è configurato in CA SDM.

   Tipo di oggetto

   Selezionare il tipo di oggetto su cui è possibile eseguire la macro.

4. Fare clic su Continua.

   La pagina viene compilata con i dati rimanenti necessari per la macro in base al tipo di macro selezionato.

   Nota: In base all'esempio, selezionare la macro Notifiche multiple (a pagina 260) come tipo di macro per inviare una notifica di posta elettronica quando si verifica una violazione di SLA. Per ulteriori informazioni sugli altri tipi di macro, consultare la *Guida in linea*.

Macro Più notifiche

Questo tipo di macro consente di inviare una notifica a uno o più contatti. Consente di specificare il messaggio da inviare, i destinatari e il livello di urgenza.

Procedere come descritto di seguito:

1. Immettere il nome del modello direttamente nel campo Modello di messaggio o fare clic sull'icona di ricerca per selezionare il modello desiderato. Questo modello viene utilizzato per creare il messaggio di notifica.
2. Fare clic su Salva.
3. Selezionare i contatti appropriati ai quali inviare la notifica dalle seguenti schede:

   Nota: Utilizzare il pulsante Aggiorna contatti visualizzato in ciascuna scheda per cercare e selezionare un numero maggiore di contatti a cui inviare la notifica.

   Contatti oggetto

   Consente di visualizzare le organizzazioni, i vendor e gli elementi della configurazione disponibili per il tipo di oggetto selezionato che riceveranno la notifica sui ticket. Ad esempio, è possibile selezionare Utente finale interessato oppure Organizzazione Utente finale interessato a cui inviare la notifica.

   Contatti

   Mostra le singole persone aggiunte alla macro di notifica, indipendentemente dalla loro associazione con il ticket.

   Tipi contatto

   Mostra gli utenti definiti all'interno della macro di notifica e con la medesima classificazione, quali l'analista o il cliente.

4. Fare clic su Salva.

   La macro notifiche multiple viene creata.

Creazione di un evento

Creare un evento e associare un marco a questo evento. L'evento viene eseguito dopo che è trascorso un determinato periodo di tempo. Se all'evento è associata una macro, viene eseguita un'azione.

Nota: in caso di installazione dell'opzione multi-tenancy, selezionare il titolare appropriato dall'elenco a discesa. L'opzione pubblica (condivisa) consente di creare l'oggetto per tutti i titolari.

Procedere come descritto di seguito:

1. Selezionare Eventi e macro, Eventi nella scheda Amministrazione.

   Viene visualizzata la pagina Elenco Eventi.

2. Fare clic su Crea Nuovo.

   Viene visualizzata la pagina Crea Nuovo evento.

3. Completare i campi relativi all'evento e le informazioni di configurazione.

   Fare clic su Salva.

4. Per aggiungere la macro a questo evento, completare le informazioni sull'azione (a pagina 263).

   Il nuovo evento viene salvato.

Ulteriori informazioni:

Campi Evento (a pagina 262)
Campi Informazioni di configurazione (a pagina 263)
Campi di Informazioni azione (a pagina 263)

Campi Evento

Completare i campi seguenti per aggiungere o modificare un evento:

Nome

Il nome dell'evento.

Tipo di oggetto

Indica se l'evento è associato a una questione, una richiesta, un ordine di cambiamento, un'attività flusso di lavoro, un documento della conoscenza, una scheda Report della conoscenza, una sessione di assistenza o un'indagine gestita.

Questo campo può essere modificato solo quando si crea un evento. Questo campo è di sola lettura quando si desidera aggiornare l'evento.

Stato record

Indica se l'evento è attivo o non attivo. È possibile utilizzare solamente gli eventi attivi.

Campi Informazioni di configurazione

Completare i campi seguenti per aggiungere o modificare le informazioni di configurazione:

Ritardo

Specifica il tempo trascorso il quale l'evento viene attivato.

Ritardo ripetizione

Specifica l'intervallo di tempo dopo il quale si desidera che l'evento venga attivato di nuovo.

Consenti reimpostazione ora

Specifica se un analista di service desk può modificare l'opzione Ritardo. È necessario che questa opzione sia selezionata affinché un evento possa essere utilizzato come un evento del tipo di servizio (un evento associato a un livello di supporto specifico, ad esempio la risoluzione in 4 ore).

Turno

Consente di specificare le date, i giorni e le ore di quando è attivo il tipo di servizio.

Flag evento terminato

Specifica l'azione da intraprendere una volta che l'evento è stato completato.

Ripeti evento

Consente di ripetere l'evento nell'intervallo di tempo specificato finché la questione non viene chiusa.

Salva cronologia

Registra la cronologia delle attività intraprese in relazione all'evento.

Nessuna cronologia

Non viene registrata alcuna cronologia eventi. L'evento non viene visualizzato nella finestra Cronologia eventi.

Condizione

Mostra la macro (se associata all'evento) che indica la condizione verificata dall'evento.

Testo

Definisce la configurazione dell'evento. Per alcune macro di azione, questo campo viene utilizzato per uno scopo specifico. Ad esempio, per la macro di azione Trasferisci a contatto evento, contiene l'ID utente della persona a cui si desidera trasferire il ticket.

Campi di Informazioni azione

Selezionare le azioni da associare all'evento nel modo seguente:

1. Fare clic sulla scheda Informazioni azione.
2. Selezionare una o entrambe le caselle di controllo Imposta violazione SLA per azioni in caso di valore True/False della macro. Se queste caselle di controllo sono abilitate, viene registrata una violazione SLA (Accordo sui Livelli di servizio) quando viene rilevata una condizione True o False per l'evento.

   Nota: Per registrare le violazioni SLA, specificare macro appropriate per la condizione True o False nell'elenco azioni.
3. Fare clic su Aggiorna azioni in caso di valore True.

   Viene visualizzata la pagina Ricerca Macro.
4. La ricerca per le macro viene eseguita se la condizione dell'evento è un valore True.
5. Selezionare le macro desiderate dall'elenco a sinistra e fare clic su Altro (>>).

   Le macro selezionate vengono aggiunte all'elenco a destra.
6. Quando tutte le macro desiderate si trovano nell'elenco a destra, fare clic su OK.

   Le macro selezionate vengono visualizzate nell'Elenco azioni in caso di valore True della macro.
7. Fare clic su Aggiorna azioni in caso di valore False e ripetere la procedura sopra riportata per selezionare le macro da eseguire se la condizione dell'evento è un valore False.

Personalizzazione di un tipo di servizio

È possibile creare un tipo di servizio che soddisfi determinati requisiti. È possibile inoltre modificare un tipo di servizio predefinito.

Procedere come descritto di seguito:

1. Selezionare Service Desk, Tipi di servizio nella scheda Amministrazione.

   Viene visualizzata la pagina Elenco Tipi di servizio.

2. Fare clic su Crea Nuovo.

   Viene visualizzata la pagina Crea Nuovo tipo di servizio.

3. In caso di installazione dell'opzione multi-tenancy, selezionare il titolare appropriato dall'elenco a discesa. L'opzione pubblica (condivisa) consente di creare l'oggetto per tutti i titolari.

4. Completare i campi seguenti:

   Simbolo

   Definisce un identificatore univoco per il tipo di servizio. In questo esempio, si assegna il simbolo 24_hr_resolution.

   Classificazione

   Definisce una classificazione per il tipo di servizio. In questo esempio, il ticket di richiesta hardware può essere associato a più tipi di servizio. Il valore della classificazione determina il tipo di servizio valido. Il tipo di servizio con una classificazione bassa ha la priorità più alta.

   Immettere 1.

   Turno

   Consente di specificare le date, i giorni e le ore di quando è attivo il tipo di servizio. Le regole seguenti sono valide per i turni:

   - Se si applica un turno a un tipo di servizio, è necessario interrompere e riavviare il servizio affinché il turno sia immediatamente attivo.
   - Se è stato specificato un turno per un tipo di servizio, ma non ne è stato specificato alcuno per l'evento, il turno del tipo di servizio è attivo.
   - Se è stato specificato un turno per un evento, ma non ne è stato specificato alcuno per un tipo di servizio, il turno del tipo di servizio non viene considerato.
   - Se è stato specificato il turno per un evento e per un tipo di servizio, il turno del tipo di servizio non viene considerato.

   Fuso orario

   Specifica il fuso orario per il tipo di servizio. Questo fuso orario è utilizzato per attivare gli eventi nel sistema qualora non sia selezionata l'opzione Usa fuso orario dell'utente finale.

Usa il fuso orario dell'utente finale

Specifica il fuso orario dell'utente finale interessato per attivare gli eventi.

Costo violazione

Specifica il costo che comporta la violazione del limite temporale del tipo di servizio.

5. Fare clic su Salva.

   Il tipo di servizio viene salvato.

6. Per associare un evento del tipo di servizio, selezionare la scheda appropriata (Richieste, Ordini di cambiamento, Attività Ordini di cambiamento, Issue o Attività Issue) e fare clic su Aggiungi evento Tipo di servizio.

   Viene visualizzata la pagina Crea Nuovo evento Tipo di servizio.

7. Fare clic su Evento.

   Viene visualizzata la pagina Elenco Eventi.

8. Eseguire una delle seguenti operazioni:

   - Selezionare Crea Nuovo per creare un evento. Completare i campi relativi all'evento e le informazioni di configurazione. Per aggiungere una macro a questo evento, completare le informazioni sull'azione (a pagina 263).

   - Selezionare uno degli eventi esistenti dall'elenco. È possibile utilizzare i criteri di filtro per cercare un evento.

     L'evento selezionato o creato viene mostrato nel campo Evento.

9. Fare clic su Continua.

   La pagina dei dettagli del tipo di servizio viene visualizzata con l'evento associato.

Associazione del tipo di servizio a un oggetto

I tipi di servizio possono essere associati a vari oggetti, ad esempio contatti, organizzazioni, categorie e codici di priorità. Secondo l'esempio, il tipo di servizio viene associato all'area Incidente (in questo caso: Hardware).

Procedere come descritto di seguito:

1. Aprire il ticket correlato a cui si desidera assegnare uno SLA.
2. Fare clic su Hardware nel campo Area Incidente.

   Viene visualizzata la pagina Aggiorna area Richiesta/Incidente/Problema Hardware).
3. Fare clic su Modifica.
4. Fare clic su Tipo di servizio.

   Viene visualizzata la pagina Elenco Tipi di servizio.
5. Cercare il tipo di servizio 24_hr_resolution creato.
6. Fare clic su 24_hr_resolution nei risultati della ricerca.

   La pagina Aggiorna area Richiesta/Incidente/Problema Hardware si apre con il tipo di servizio aggiornato.
7. Fare clic su Salva.

   Il tipo di servizio viene associato all'area degli Incidenti Hardware.

Ritardo o ripresa di un evento tipo servizio

È possibile ritardare e riprendere eventi tipo servizio.

Per ritardare un evento

1. Selezionare il ticket richiesto dalla pagina di elenco nella scheda Service Desk.

   Viene visualizzata la pagina dei dettagli del ticket.

2. Fare clic sulla scheda Tipo servizio.

   Viene visualizzato un elenco di tutti gli eventi tipo di servizio aggiunti al ticket.

3. Fare clic su Ritardo.

   Viene visualizzata la pagina Motivo.

4. Immettere il motivo del ritardo dell'evento, quindi fare clic su OK.

   Nella pagina dei dettagli del ticket lo stato dell'evento compare come Posticipato.

Per riprendere un evento

1. Selezionare il ticket richiesto dalla pagina di elenco nella scheda Service Desk.

   Viene visualizzata la pagina dei dettagli del ticket.

2. Fare clic sulla scheda Tipo servizio.

   Viene visualizzato un elenco di tutti gli eventi tipo di servizio aggiunti al ticket.

3. Fare clic su Riprendi.

   Viene visualizzata la pagina Motivo.

4. Immettere il motivo della ripresa dell'evento, quindi fare clic su OK.

   Nella pagina dei dettagli del ticket lo stato dell'evento compare come In sospeso.

Creazione delle destinazioni del servizio

Per ridurre al minimo le violazioni degli accordi di servizio (SLA), è possibile creare un insieme di modelli di destinazione del servizio per misurare ogni fase della risoluzione di un ticket. Analogamente ai tipi di servizio, ogni destinazione servizio contiene una condizione e il tempo di completamento stimato. Le destinazioni servizio non forniscono tuttavia alcun meccanismo di azione.

Durante la creazione di un ticket, un tipo di servizio assegna al ticket una o più destinazioni di servizio che consentono di tenere traccia di ogni fase della risoluzione del ticket. Ogni volta che il ticket viene modificata, le destinazioni di servizio attive valutano la rispettiva condizione. Se la condizione è soddisfatta, il ticket e il registro attività mostrano il tempo di completamento effettivo. Quando il tempo supera quello stimato, il ticket visualizza di quanto tempo è stata mancata la destinazione.

Le destinazioni servizio consentono di effettuare le seguenti operazioni:

- Verificare che i ticket dello stesso Tipo servizio seguano le stesse destinazioni servizio.
- Monitorare se i ticket vengono chiusi nei tempi richiesti.
- Visualizzare informazioni, quali il numero residuo di minuti al completamento di una destinazione servizio.

Durante la creazione di modelli di destinazione servizio, si consideri quanto segue:

- Considerare il risultato richiesto per soddisfare la destinazione servizio. Utilizzare una macro condizionale esistente o una macro condizionale definita dal sito per valutare i dati del ticket. Se necessario, personalizzare o scrivere una nuova macro per gestire la destinazione di servizio.
- Calcolare la violazione prevista e i costi di penalità in base agli accordi SLA.
- Assegnare almeno un modello di destinazione servizio a un Tipo servizio.

Procedere come descritto di seguito:

1. Creare un modello di destinazione di servizio (a pagina 270) per la gestione di Richieste, Incidenti, Problemi, Ordini di cambiamento o Questioni.
2. Collegare il modello di destinazione servizio a un tipo di servizio (a pagina 271).
3. Assegnare i dettagli del modello di destinazione servizio a una categoria di ticket, ad esempio ticket richiesta, incidente, problema, ordine di cambiamento o questione.

   Al momento della creazione del ticket, il modello appropriato viene associato automaticamente al ticket in base al rispettivo Tipo servizio. Ogni volta che un utente crea un ticket, lo stato della destinazione servizio viene automaticamente visualizzato nella scheda Tipo servizio.

Creazione di un modello di destinazione servizio.

È possibile creare un modello destinazione servizio per misurare destinazioni di servizio per richieste, incidenti, problemi, questioni o ordini di cambiamento. Dopo aver creato il modello, è possibile collegarlo a un tipo di servizio.

Nota: se è installata l'opzione multi-tenancy, specificare il titolare nel campo Titolare.

Procedere come descritto di seguito:

1. Selezionare Service Desk, Modelli di destinazione servizio nella scheda Amministrazione.

   Viene visualizzata la pagina Elenco modelli Destinazione servizio.

2. Fare clic su Crea Nuovo.

   Viene visualizzata la pagina Crea Nuovo modello Destinazione servizio.

3. Selezionare un tipo di ticket dal campo Tipo di oggetto e fare clic su Continua.

4. Completare i campi seguenti in modo appropriato:

   Nome

   Definisce un identificatore descrittivo per una destinazione servizio.

   Tipo di oggetto

   Identifica il tipo di ticket per la destinazione servizio.

   Durata destinazione

   Specifica il tempo massimo per il completamento della destinazione servizio nel formato hh:mm:ss.

   Turno

   Specifica il turno contenente l'intervallo di ore lavorative utilizzato per il calcolo delle ore per la destinazione di servizio, ad esempio L-V 08.00-17.00.

   Costo

   Definisce informazioni come la stima del costo associato al mancato raggiungimento della destinazione servizio.

   Stato record

   Indica se la destinazione è attiva o non attiva.

   Condizione

   Specifica il nome della condizione (macro o condizione definita dal sito) che valuta i dati di ticket e determina se la destinazione servizio è stata raggiunta.

   Risultato richiesto

   Specifica un valore Vero o Falso che indica se la destinazione di servizio è completa.

Consenti reimpostazione data/ora effettiva

Specifica se consentire agli utenti di impostare la data e l'ora per una destinazione servizio.

Consenti reimpostazione data/ora effettiva

Specifica se consentire agli utenti di reimpostare la data e l'ora per una destinazione servizio.

5. Fare clic su Salva.

   Il modello della destinazione servizio viene creato.

Collegare un Modello di destinazione servizio a un Tipo servizio

Quando si collega un modello di destinazione servizio a un tipo servizio, le destinazioni vengono automaticamente collegate a un ticket al momento dell'assegnazione del tipo servizio. È possibile assegnare un modello di destinazione servizio una sola volta a un tipo servizio. Più destinazioni di servizio diverse possono essere collegate a un tipo servizio.

Procedere come descritto di seguito:

1. Selezionare Service Desk, Tipi di servizio nella scheda Amministrazione.

   Viene visualizzata la pagina Elenco Tipi di servizio.

2. Selezionare un tipo servizio.

   Viene visualizzata la pagina Dettagli Tipo di servizio.

3. Selezionare la scheda di destinazione per il tipo di oggetto selezionato. Ad esempio, se si è creata la destinazione di servizio per la richiesta, selezionare la scheda Destinazioni Richiesta per gestire i ticket del problema, incidente e richiesta.

4. Fare clic su Collega modello destinazione servizio.

   Viene visualizzata la pagina Crea nuovo modello Destinazione servizio collegato.

5. È possibile immettere un valore direttamente o fare clic sulla lente di ingrandimento per cercare il tipo di servizio.

6. Fare clic su Continua.

7. Fare modifiche al modello della destinazione servizio, se necessario.

8. Fare clic su Salva.

   Il modello della destinazione servizio è collegato al tipo di servizio.

Visualizzazione di contatori e timer per le destinazioni servizio

Se un analista ha assegnato un insieme di destinazioni servizio a un ticket, è possibile visualizzare lo stato e le scadenze per il completamento di ciascuna destinazione.

Per visualizzare contatori e timer del ticket per una destinazione servizio

1. Nella scheda Service Desk visualizzare un elenco di incidenti, problemi, richieste, ordini di cambiamento o questioni.

   Viene visualizzata la pagina dei dettagli del ticket.

2. Fare clic sulla scheda Tipo servizio.

   Ulteriori informazioni sul tipo di servizio vengono visualizzate nella parte inferiore del ticket.

3. Nella colonna Destinazione, fare clic sulla destinazione servizio per ottenere maggiori informazioni.

   Nella parte inferiore dalla pagina Dettagli destinazione servizio viene visualizzata la sezione Timer e contatori del ticket. Nella pagina Dettagli destinazione servizio vengono visualizzati i campi seguenti:

   Nome

   Consente di visualizzare il nome della destinazione servizio.

   Durata destinazione

   Visualizza il tempo disponibile assegnato per eseguire la destinazione servizio. È possibile ignorare questo valore solo modificando il ticket.

   Turno

   Visualizza la pianificazione utilizzata per calcolare i tempi per la destinazione servizio.

   Condizione

   Visualizza la macro condizionale o la macro condizionale definita dal sito che valuta i dati del ticket per stabilire se il lavoro può essere concluso entro i tempi di destinazione servizio stabiliti.

   Risultato richiesto

   Visualizza il risultato richiesto della condizione o della macro condizionale definita dal sito.

   Costo

   Visualizza la penalità in cui si incorre per aver mancato la destinazione. Queste informazioni vengono visualizzate anche sul ticket.

   Data/Ora di destinazione

   Visualizza la scadenza per il completamento della destinazione. Se il ticket si trova in stato In attesa oppure la destinazione servizio è stata raggiunta, questo campo è vuoto.

Data/ora effettiva

Specifica la data e l'ora in cui la condizione è stata soddisfatta oppure in cui l'utente ha fatto clic su Imposta data/ora effettiva.

Tempo residuo

Visualizza il tempo rimanente per la destinazione servizio. Un valore negativo indica il tempo in eccesso rispetto al periodo di tempo stabilito.

Consenti reimpostazione data/ora effettiva

Specifica se è possibile impostare la data/ora effettiva. Sì indica che è possibile impostare la Data/ora effettiva della destinazione servizio. No indica che non è possibile sovrascrivere il valore Data/ora effettiva.

Consenti reimpostazione data/ora effettiva

Specifica se è possibile riavviare la data/ora. Sì indica che è possibile reimpostare la Data/ora effettiva della destinazione servizio. No indica che non è possibile reimpostare il valore Data/ora effettiva.

Data/Ora ultima modifica

Visualizza la data dell'ultima modifica del ticket.

Autore ultima modifica

Visualizza il nome dell'ultima persona che ha modificato il ticket.

Tipo servizio

Visualizza il nome del tipo di servizio associato alla destinazione servizio.

Modello Destinazione servizio

Visualizza il nome del modello di destinazione servizio collegato al tipo di servizio utilizzato per creare la destinazione servizio.

Blocco Ora/Data di destinazione da

Impedisce alla data/ora di destinazione di essere automaticamente aggiornata quando lo stato del ticket diventa In attesa oppure quando il ticket viene ritardato.

Data/Ora ultimo avvio

Visualizza la data/ora in cui è stato avviato per l'ultima volta il timer della destinazione servizio.

Stato ticket

Visualizza il valore del campo Stato del ticket.

Stato sospensione

Specifica se lo stato del ticket ha messo il ticket in attesa.

Data/Ora ultima sospensione

Visualizza la data/ora in cui il ticket è stato messo in attesa.

Sospendi conteggio

Visualizza quante volte il ticket è stato messo in attesa.

Data/Ora ultima risoluzione

Visualizza la data/ora in cui il ticket è passato per l'ultima volta allo stato Risolto.

Conteggio risolto

Visualizza quante volte il ticket è passato allo stato Risolto.

Data/Ora ultima chiusura

Visualizza la data/ora in cui il ticket è passato per l'ultima volta allo stato Chiuso.

Conteggio chiuso

Visualizza quante volte il ticket è passato allo stato Chiuso.

Data/Ora di apertura del ticket

Indica la data e l'ora in cui il ticket è stato aperto.

Data/Ora di risoluzione del ticket

Indica la data e l'ora in cui il ticket è stato risolto.

Data/Ora chiusura del ticket

Indica la data e l'ora in cui il ticket è stato chiuso.

Visualizzazione dello stato della destinazione servizio

In un ticket aperto è possibile visualizzare lo stato relativo a una destinazione servizio. Le informazione di stato, quali Tempo residuo e Costo violazione, consentono di attribuire delle priorità al proprio lavoro.

Per visualizzare lo stato di un destinazione servizio

1. Nella scheda Service Desk visualizzare un elenco di incidenti, problemi, richieste, ordini di cambiamento o questioni.

   Nell'elenco ticket selezionato vengono visualizzate le seguenti informazioni sulle destinazioni servizio:

   Destinazione servizio

   Visualizza data e ora in cui scade la prossima destinazione servizio.

   Violazione prevista

   Visualizza il costo in cui si incorre violando il limite temporale del tipo di servizio.

2. Selezionare il ticket desiderato dalla pagina elenco.

   Viene visualizzata la pagina dei dettagli del ticket.

3. Fare clic sulla scheda Tipo servizio.

   Nota: le destinazioni di servizio vengono visualizzate nei ticket che soddisfano le condizioni impostate dall'amministratore. Il calcolo automatico della priorità può influire sul modo in cui vengono calcolate e visualizzate le informazioni di destinazione.

   Se il ticket soddisfa condizioni di destinazione predefinite, nell'elenco delle destinazioni servizio vengono visualizzate le seguenti informazioni:

   Azione

   Imposta o reimposta Data/ora effettiva sulla data e ora correnti.

   Destinazione

   Specifica la destinazione servizio corrente per il ticket.

   Data/Ora di destinazione

   Specifica la data e l'ora in cui scade la destinazione servizio. Se lo stato del ticket è In attesa, questo valore è vuoto.

   Data/ora effettiva

   Specifica l'ora in cui la condizione di destinazione è stata soddisfatta. Se non viene visualizzato alcun valore, la condizione di destinazione non è stata soddisfatta.

   Tempo residuo

Specifica il tempo residuo per la destinazione servizio quando il ticket è in attesa. Se la destinazione servizio è stata soddisfatta, Tempo residuo mostra il tempo non utilizzato. Un valore negativo indica il tempo trascorso dalla data di destinazione mancata.

Costo violazione

Visualizza la penalità in cui si incorre per aver mancato la destinazione. Queste informazioni vengono visualizzate anche sul ticket.

Contratti del servizio

Il modello SLA include il contratto di assistenza. Il contratto di assistenza definisce lo SLA per una specifica organizzazione, inclusi i tipi di servizio, le aree Richiesta e le categorie Issue o le categorie Cambiamento. A tali definizioni viene fatto riferimento come categorie *private* e tipi di servizio *privati*.

Nota: le categorie e i tipi di servizio *privati* possono essere utilizzati solo nei ticket in cui è in vigore il contratto di assistenza.

Il contratto di assistenza valido per un ticket è determinato dall'*organizzazione interessata* del ticket, ovvero l'organizzazione dell'utente finale interessato (si tratta del campo Organizzazione in un record di contatto). Per il ticket è possibile selezionare solo le aree o le categorie elencate nel contratto di assistenza. Inoltre, i soli tipi di servizio che possono essere applicati sono quelli *privati* elencati nel contratto. Ciò garantisce che gli SLA relativi ad un'organizzazione non vengano accidentalmente combinati con quelli di altre organizzazioni.

Inoltre, un contratto di assistenza associa i tipi di servizio ai campi di riferimento comuni in un ticket, ad esempio i campi Priorità e Asset. Questa associazione riguarda i tipi di servizio e gli attributi di un ticket. Il contratto di un'organizzazione può ad esempio assegnare i tipi di servizio ad ognuno dei cinque oggetti Priorità. Quando viene creato un ticket con una determinata priorità, viene applicato il tipo di servizio associato.

Le categorie e i tipi di servizio possono essere definiti esternamente ad un contratto e in questo caso vengono considerati *pubblici*. Le definizioni pubbliche vengono utilizzate quando per un ticket non è in vigore alcun contratto di assistenza. L'assenza di un contratto di assistenza può verificarsi se l'utente finale non appartiene ad un'organizzazione o il contratto dell'organizzazione non è attivo. Una definizione pubblica è un meccanismo utile di backup o predefinito. I tipi di servizio pubblici vengono impostati direttamente nelle categorie e in altri campi di riferimento.

Tutti i tipi di servizio applicabili vengono assegnati al ticket. Ciò garantisce che tutti gli aspetti di uno SLA siano visibili e applicati, ad esempio:

- Una stampante può presentare un tipo di servizio che richiede l'invio di un tecnico entro 2 giorni.
- Un tipo di servizio dell'oggetto Priorità può richiedere una richiamata entro un'ora.

Quando questi due tipi di servizio sono impostati, tali azioni vengono applicate.

Il tracciamento di più tipi di servizio facilita anche l'assegnazione della priorità ai ticket. Ad esempio, il tipo di servizio assegnato per un ticket riguardante una tastiera rotta ha una priorità bassa. Se invece l'utente finale interessato necessita urgentemente della tastiera, la priorità del servizio può essere aumentata.

Nota: il modello SLA viene applicato per impostazione predefinita. Con le versioni precedenti di CA SDM era possibile associare un solo tipo di servizio a un ticket. La selezione del tipo di servizio richiedeva la ricerca del tipo con *classificazione* più alta tra tutti i tipi di servizio possibili. Il modello che utilizza lo schema di classificazione potrebbe ancora essere utilizzato installando l'opzione 'classic_sla_processing'.

Migrazione dei contratti di assistenza

Se CA SDM viene installato come migrazione, l'opzione classic_sla_processing viene attivata per impostazione predefinita in modo che l'elaborazione SLA possa continuare normalmente. Questo fornisce il tempo necessario per la creazione dei contratti di assistenza appropriati ed eventualmente per la disattivazione dell'opzione classic_sla_processing.

Quando si generano i contratti di assistenza, non è necessario creare tipi di servizio, aree richiesta o categorie. È possibile utilizzare il pulsante Copia, presente in Dettagli contratto di assistenza, per copiare oggetti esistenti nel contratto.

Se nell'installazione precedente il campo support_lev era contrassegnato come obbligatorio per qualsiasi tipo di ticket, questa limitazione deve essere rimossa. Il campo support_lev continua ad essere presente ma nel modello corrente non è impostato, con conseguente generazione di un errore di campo obbligatorio con i nuovi ticket. Questo riguarda gli oggetti Richiesta (cr), Questione (iss) oppure Ordine di cambiamento (chg).

Ora violazione

Quando è in uso il modello SLA, il sistema Ora violazione di CA SDM consente di tenere traccia e di assegnare la priorità ai ticket in base all'ora della violazione prevista. Questo sistema monitora tutti i ticket attivi e imposta l'ora della violazione prevista per ciascun tipo di servizio. È ora possibile segnalare e ordinare i ticket in base all'ora e al costo della violazione e risolvere prima le questioni più urgenti e onerose.

Il sistema Ora violazione monitora tutti i ticket attivi e valuta i relativi eventi SLA in modo invisibile all'utente, determinando quali eventi imposteranno il flag di violazione SLA. Gli eventi non vengono eseguiti ma il sistema esamina l'esito di ciascun evento in base allo stato corrente del ticket. Se la valutazione causa l'impostazione del flag di violazione SLA, il tipo di servizio associato del ticket viene aggiornato con un valore Ora violazione. Questo valore rappresenta la data/ora di attivazione dell'evento che a sua volta imposta la violazione SLA.

La valutazione si verifica non appena un ticket viene inserito o aggiornato. Poiché i ticket vengono spesso aggiornati in rapida successione, la valutazione viene visualizzata per un breve periodo. Tale ritardo viene controllato dall'opzione ttv_evaluation_delay. Trascorso il periodo di ritardo, la funzione Ora violazione valuta tutti gli eventi SLA che possono impostare il flag di violazione SLA.

Ogni evento presenta una condizione facoltativa e un set di azioni (macro) che vengono avviate in base all'esito della condizione. Per garantire prestazioni adeguate, le informazioni sul modello evento vengono inserite nella cache dalla funzione Ora violazione e periodicamente aggiornate. Le proiezioni eseguite dalla funzione Ora violazione che includono i modelli evento aggiornati di recente potrebbero non essere precise per alcuni minuti.

Nota: le proiezioni della funzione Ora violazione vengono riportate nella scheda Tipo servizio di ciascun ticket. La funzione Ora violazione viene attivata con l'opzione ttv_enabled.

Fusi orari e turni

Per soddisfare i complessi requisiti relativi all'esecuzione automatica delle applicazioni aziendali, CA SDM consente di definire i fusi orari e i turni in base alle proprie esigenze e di registrarli in modo da poterli consultare rapidamente.

- I fusi orari identificano il fuso orario in cui si trovano l'utente, l'elemento della configurazione ecc.
- I turni definiscono il periodo durante il quale il monitoraggio dell'evento, le ore di lavoro di un tipo di servizio o lo SLA sono in vigore.

La possibilità di determinare una linea di condotta in base al momento in cui si verifica l'evento può essere di fondamentale importanza per la corretta gestione dell'evento. I fusi orari e i turni definiti possono essere utilizzati da qualunque funzione di CA SDM.

Ulteriori informazioni:

Configurazione dei turni (a pagina 281)
Fusi orari (a pagina 453)

Configurazione dei fusi orari

I codici dei fusi orari definiscono il fuso orario dal quale solitamente un utente accede al sistema (ovvero, il fuso orario locale dell'utente) oppure il fuso orario in cui si trova un elemento della configurazione. Gli orari lavorativi vengono sempre immessi in base al fuso orario del server CA SDM. Questo significa che gli orari lavorativi possono essere sempre confrontati uniformemente.

I fusi orari vengono utilizzati per gestire i tipi di servizio, le operazioni di escalation e la risposta complessiva nei confronti degli utenti finali in base alla capacità di CA SDM di presentare l'orario corretto per più fusi orari. CA SDM regola automaticamente la differenza tra il fuso orario in cui l'utente ha eseguito l'accesso o in cui si trova l'elemento della configurazione e il fuso orario in cui il server è in esecuzione. I fusi orari utilizzano il formato GMT (Greenwich Mean Time).

Nota: per informazioni su come definire i fusi orari, vedere la *Guida in linea*.

Modalità di gestione di più fusi orari per i tipi di servizio

I server e gli utenti di CA SDM possono trovarsi in località con fusi orari diversi. Per la differenza di fuso orario, è possibile che vengano ignorate date e ore di scadenza di tipi di servizio.

Per correggere la differenza di fuso orario, è possibile configurare CA SDM affinché visualizzi le ore di scadenza dei tipi di servizio nell'ora del fuso orario dell'utente finale. Se due utenti in località con fusi orari diversi visualizzano lo stesso ticket, ogni utente vede i valori Ora di scadenza espressi nell'ora del fuso orario locale. Tuttavia, i valori Ora di avvio rispecchiano sempre il fuso orario del server.

Per configurare la gestione del fuso orario dell'utente finale, procedere come segue:

1. Creare un codice server che identifichi il nome server e il relativo fuso orario.
2. Creare o aggiornare un tipo di servizio. Impostare il campo Usa il fuso orario dell'utente finale su Sì.

   Impostando questo campo su Sì, l'Ora di scadenza viene visualizzata e aggiornata in base al fuso orario dell'utente finale.

Esempio: visualizzazione delle date di scadenza dei tipi di servizio in base al fuso orario dell'utente finale

Nell'esempio seguente si configura CA SDM per visualizzare le date di scadenza del Tipo servizio in base al fuso orario dell'utente finale. Server e utente sono su computer separati e in località con fuso orario diverso.

Per creare un codice server che identifichi il nome server e il relativo fuso orario

1. Nella scheda Amministrazione sul server host, selezionare Service Desk, Codice applicazione.
2. Fare clic su Codici, Server.

   Viene visualizzato l'elenco Server.
3. Fare clic sul server Host locale.

   Viene visualizzata la pagina Dettagli nome server .
4. Impostare il fuso orario. Ad esempio, impostare il fuso orario su GMT (EU). Il nome dell'host locale deve corrispondere al valore NX_LOCAL_HOST archiviato nel file NX.env per il server.
5. Fare clic su Salva.

   Il server host utilizza ora il nuovo fuso orario. Quando l'utente visualizza un ticket, l'Ora di avvio rispecchia il fuso orario del server.

Per creare un tipo di servizio

1. Nella scheda Amministrazione, selezionare Tipi di servizio.

Viene visualizzato l'elenco dei tipi di servizio.

2. Fare clic su Risoluzione - Priorità 1 o su un altro tipo di servizio che gestisce richieste con priorità 1.

   Viene visualizzata la pagina Aggiorna tipo servizio.

3. Selezionare la casella di controllo Usa il fuso orario dell'utente finale.

4. Fare clic su Salva.

   Il record del tipo di servizio viene aggiornato.

Per visualizzare i fusi orari sul ticket

1. Su un altro computer, aprire un ticket Richiesta e impostare la Priorità su 1.

   Nota: se si utilizzano destinazioni servizio, impostare i valori nel ticket affinché la destinazione utilizzi la Risoluzione - Priorità 1.

2. Visualizzare il ticket e fare clic sulla scheda Tipo servizio.

   L'Ora di avvio rispecchia il fuso orario del server. L'Ora di scadenza rispecchia l'ora sul computer locale dell'utente finale.

3. Chiudere la pagina che visualizzare il ticket Richiesta.

4. Modificare il fuso orario sul computer locale dell'utente finale.

5. Visualizzare il Tipo servizio del ticket sul computer locale dell'utente finale per vedere i valori Ora di scadenza corrispondenti basati sul fuso orario dell'utente.

   L'Ora di scadenza rispecchio il nuovo fuso orario.

Nota: per informazioni dettagliate sui tipi di server o sui codici server, consultare la *Guida in linea*.

Configurazione dei turni

I turni identificano i giorni, le date e gli orari in cui un evento o una pianificazione sono in vigore. È possibile specificare i giorni o le date oppure i giorni e le date. Specificare l'ora è facoltativo.

Nota: per informazioni su come definire i turni, vedere la *Guida in linea*.

Quando si monitorano gli eventi per i ticket, i turni definiscono quando l'evento è monitorato o, in altre parole, quando il turno è in vigore. Ad esempio, utilizzando l'evento predefinito Pri 1 e attiva - Notif assegn quest, se una questione con priorità 1 viene aperta alle 16:45 e la pianificazione del turno è dalle 9:00 alle 17:00, l'evento monitorato invia automaticamente la notifica all'assegnatario della questione alle 9:45 del giorno successivo.

Nota: i turni vengono utilizzati anche per l'assegnazione automatica dei ticket ai contatti.

Ulteriori informazioni:

Definizione della struttura di supporto (a pagina 385)

Protezione

Prima di consentire l'utilizzo di CA SDM, è fondamentale configurare la protezione per determinare quanto segue:

- Gli utenti che hanno accesso al sistema
- Il livello di accesso per ciascun utente
- Le modalità di autenticazione degli utenti all'accesso

Nota: per informazioni dettagliate sulla modalità di esecuzione delle attività di amministrazione della protezione, vedere la *Guida in linea*.

Configurazioni della base utenti di CA EEM e CA Workflow

CA EEM è un repository centrale delle informazioni utente (identità). CA EEM definisce l'autenticazione e l'accesso degli utenti ad altre applicazioni. Se sul sistema in uso sono installati più prodotti <CA>, alcuni di essi potrebbero utilizzare <EEM> per memorizzare le identità e le policy di accesso. CA SDM utilizza solo CA EEM per l'autenticazione. CA EEM non è un'opzione di configurazione di CA SDM e deve essere installato separatamente.

Il repository CA EEM dei record utente è rappresentato da *una* delle origini seguenti:

- Una directory LDAP esterna.
- Le tabelle interne di MDB.

CA EEM presenta un'interfaccia LDAP da utilizzare quando è configurato per l'uso di MDB.

Nota: le tabelle MDB utilizzate da CA EEM sono diverse da quelle utilizzate da CA SDM.

Se l'organizzazione utilizza un server directory, come ad esempio Active Directory o eTrust Directory, occorre valutare l'eventualità di configurare CA EEM in modo tale che ne utilizzi la directory per la sua base utenti. Impostando questa configurazione gli utenti della directory sono raggiungibili da qualsiasi altra applicazione che utilizzi CA EEM. Poiché CA EEM centralizza la gestione degli accessi, solitamente viene installato su un solo server.

Nota: per ulteriori informazioni sull'installazione, consultare la *Guida all'implementazione*.

CA Workflow

Durante l'installazione di CA SDM, è possibile installare facoltativamente CA Workflow, ovvero un modulo del flusso di lavoro incorporato. Poiché CA Workflow utilizza CA EEM per tutte le informazioni dell'utente, CA EEM gestisce tutti i tentativi di autenticazione e determinate autorizzazioni. CA Workflow non riconosce i record contatto di CA SDM.

Nota: per informazioni sulla configurazione dell'accesso a CA Workflow, consultare la *Guida all'implementazione*.

CA SDM

CA SDM memorizza le informazioni sul contatto nelle tabelle MDB. Queste tabelle non hanno alcuna relazione con CA EEM. CA SDM non utilizza CA EEM per la gestione dell'accesso o dell'identità. CA SDM gestisce i propri accessi e la protezione attraverso i tipi di accesso e le partizioni dati.

CA SDM utilizza solo CA EEM per l'autenticazione. Se si desidera utilizzare CA EEM per l'autenticazione di utenti in CA SDM, installare CA EEM. Se si integra CA SDM con CA EEM, sostituisce l'autenticazione del sistema operativo CA SDM con l'autenticazione CA EEM.

Nota: per informazioni sull'installazione di CA EEM, consultare la *Guida all'implementazione*. Per integrare CA EEM e CA SDM, è necessario impostare le opzioni *eiam_hostname*, *use_eiam_artifact* e *use_eiam_authentication* in Gestione opzioni, Protezione. Per ulteriori informazioni sulle opzioni, consultare la *Guida in linea*.

La base utenti di CA SDM è distinta da quella di CA EEM e di conseguenza dalla base utenti di CA Workflow. Il vantaggio dell'utilizzo di CA Workflow è rappresentato dal fatto che utenti esterni a CA SDM possono aggiungervi e completare elementi del flusso di lavoro. Ciò è utile quando CA EEM fa riferimento al server LDAP dell'organizzazione.

La sfida consiste nell'integrazione di CA SDM. Un elemento di lavoro non può essere assegnato direttamente al record contatto effettivo in CA SDM. L'assegnazione dell'elemento di lavoro ai contatti di CA SDM può essere eseguita se si verificano le seguenti condizioni:

- Il contatto CA SDM presenta un record corrispondente in CA EEM
- Tali record presentano ID utente corrispondenti.

In sintesi:

- CA SDM utilizza l'MDB per memorizzare le informazioni sul contatto. CA SDM rappresenta anche un'integrazione di LDAP per la creazione di nuovi contatti da un server LDAP e per la sincronizzazione dei contatti esistenti con la directory.
- CA EEM è la soluzione di CA per la gestione centralizzata degli utenti. Se sul sistema in uso sono installati più prodotti CA, è possibile che tutti utilizzino CA EEM per memorizzare le identità e le policy di accesso.

- CA EEM può essere configurato per puntare ad una directory esterna (LDAP) oppure utilizzare MDB per memorizzare le informazioni dell'utente. CA EEM stesso presenta un'interfaccia LDAP da utilizzare quando è configurato per l'uso di MDB.

  Nota: le tabelle utilizzate da CA EEM in MDB sono differenti da quelle utilizzate da CA SDM.

- CA Workflow utilizza sempre CA EEM per l'autenticazione utente e per la memorizzazione delle informazioni utente. Gli elementi di lavoro possono essere assegnati solo agli utenti noti a CA EEM e solo gli utenti definiti da CA EEM possono accedere all'interfaccia utente Web IDE ed Elenco di lavoro di CA Workflow.

Gli argomenti seguenti illustrano le varie opzioni di configurazione per i prodotti e in che modo tali opzioni interessino l'integrazione di CA SDM e di CA Workflow. La scelta della configurazione dipende dall'utilizzo che si intende fare di CA Workflow e dall'eventuale utilizzo di un server LDAP.

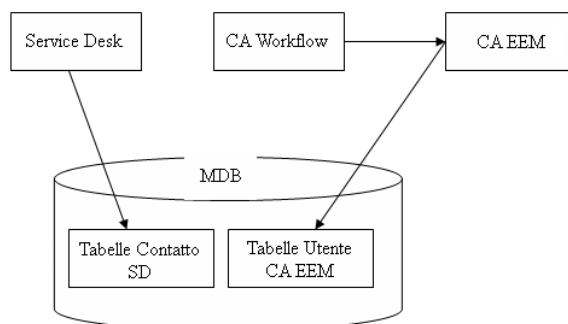
Ulteriori informazioni:

Configurazioni della base utenti di CA EEM e CA Workflow (a pagina 282)
Configurazione di CA EEM come LDAP (a pagina 286)

Configurazione predefinita

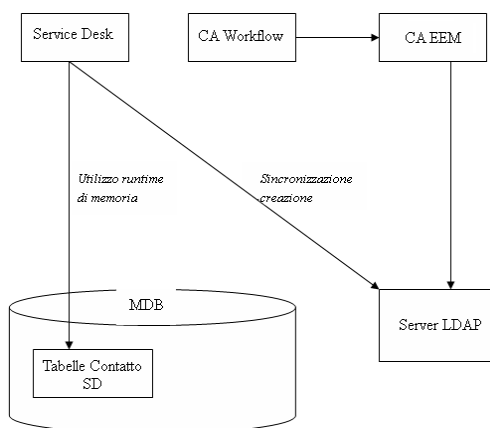
CA SDM e CA Workflow memorizzano le informazioni dell'utente dopo un'installazione predefinita come illustrato di seguito.

- CA SDM memorizza le informazioni dell'utente nelle tabelle dei contatti di CA SDM in MDB.
- CA Workflow utilizza CA EEM per memorizzare le informazioni dell'utente nelle tabelle degli utenti CA EEM in MDB.

Nel seguente diagramma viene illustrato dove vengono memorizzate le informazioni dell'utente per i prodotti:

Utilizzare la configurazione predefinita se il sito utilizza in minima parte o non utilizza affatto CA Workflow o un server directory LDAP. Questa configurazione presenta alcuni problemi. Ogni utente CA Workflow richiede un record utente CA EEM.

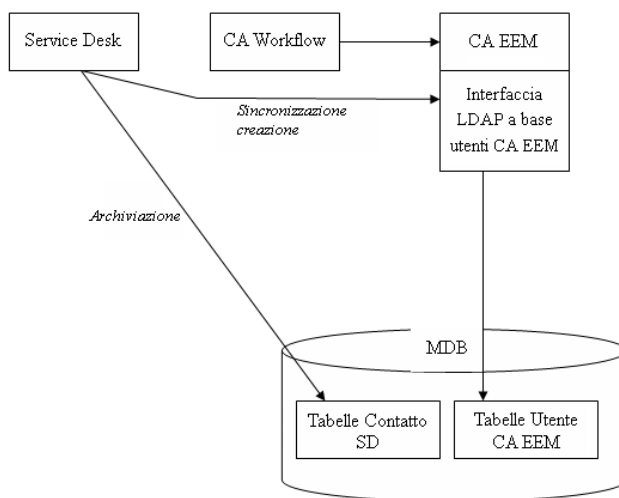
Configurazione dei server LDAP esterni

L'amministrazione dei contatti viene semplificata se CA SDM e CA Workflow utilizzano lo stesso server directory LDAP. Questa configurazione è particolarmente utile se il sito utilizza già un server LDAP come directory principale per gli utenti. Grazie alle funzionalità LDAP di CA SDM, gli ID utente dei record contatto corrispondono a quelli presenti nella directory. Ciò consente un'agevole assegnazione degli elementi di lavoro agli analisti di CA SDM. Le integrazioni diventano ancora più trasparenti se CA SDM utilizza CA EEM per l'autenticazione.

Nel seguente diagramma viene illustrato uno scenario in cui tutti gli utenti della directory LDAP accedono automaticamente all'applicazione Web Elenco di lavoro CA Workflow. CA SDM utilizza ancora le tabelle dei contatti in MDB per i relativi record utente, ma tali record possono essere importati e periodicamente sincronizzati con i record del server LDAP.

Ulteriori informazioni:

Dati di directory LDAP (a pagina 326)

Configurazione di CA EEM come LDAP

Quando CA EEM viene configurato per utilizzare MDB, anziché una directory esterna per memorizzare le informazioni dell'utente, CA EEM espone la directory dell'utente utilizzando un'interfaccia LDAP. Se il sito non utilizza un server LDAP esterno, è possibile sfruttare i vantaggi della configurazione LDAP esterna configurando CA SDM per l'utilizzo di CA EEM come origine LDAP. Questa configurazione può essere utile se il sito non utilizza un server LDAP, ma si desidera comunque consolidare la gestione degli utenti in CA EEM. Altri prodotti CA utilizzano CA EEM, che può notevolmente semplificare la gestione degli utenti.

Nota: tale configurazione è valida solo quando CA EEM è impostato per l'utilizzo di MDB. Se CA EEM viene configurato per un server LDAP esterno, configurare CA SDM affinché punti allo stesso server LDAP e *non* al server CA EEM.

Aggiornamento

Se si sta eseguendo l'aggiornamento da una versione precedente di CA SDM oppure si sta eseguendo il caricamento in batch di molti record contatto, è necessario aggiungere manualmente gli utenti a CA EEM per consentirgli l'accesso a CA Workflow.

Configurazione dell'archivio utenti di CA EEM r8.4 SP4 CR05

È possibile configurare CA EEM r8.4 SP4 CR05 per l'archiviazione dei record utente in una directory LDAP esterna o nelle relative tabelle MDB interne. Quando CA EEM utilizza una directory LDAP esterna, l'interfaccia è di sola lettura. Quindi, non è possibile aggiungere o modificare gli utenti tramite l'interfaccia CA EEM.

Procedere come descritto di seguito:

1. Fare clic su Start, Programmi, CA, Embedded Entitlements Manager, EEM UI.

   Viene visualizzata l'interfaccia utente di CA EEM.

2. Fare clic sulla scheda Configura.
3. Fare clic sulla scheda secondaria EEM Server
4. Nel riquadro di sinistra selezionare il collegamento Utenti globali/Gruppi globali.
5. Nel riquadro di destra selezionare una delle seguenti opzioni:
   - Archivia in archivio dati interno
   - Riferimento da una directory esterna
   - Riferimento da CA SiteMinder

     Nota: se si seleziona l'opzione Riferimento da una directory esterna, sarà necessario specificare i dettagli del server LDAP.

6. Fare clic su Salva.

   La configurazione dell'archivio utenti di CA EEM è completata.

   Nota: per ulteriori informazioni su CA EEM, consultare la *Guida in linea* di EEM.

Configurazione dell'archivio utenti di CA EEM r12 CR02

È possibile configurare CA EEM r12 CR02 per l'archiviazione dei record utente in una directory LDAP esterna o nelle tabelle MDB interne. Quando CA EEM utilizza una directory LDAP esterna, l'interfaccia viene visualizzata in sola lettura, pertanto non è possibile aggiungere o modificare gli utenti tramite l'interfaccia CA EEM.

Procedere come descritto di seguito:

1. Fare clic su Start, Programmi, CA, Embedded Entitlements Manager, Admin UI.

   Viene visualizzata l'interfaccia utente di CA EEM.

2. Fare clic sulla scheda Configura.
3. Fare clic su scheda secondaria User Store (Archivio utenti).
4. Nel riquadro di sinistra, fare clic sul collegamento all'archivio utenti.

5. Nel riquadro di destra selezionare una delle seguenti opzioni:
   - Store in internal user store (Archivia nell'archivio utenti interno)
   - Reference from an external LDAP Directory (Riferimento da una directory LDAP esterna)
   - Riferimento da CA SiteMinder

     Nota: se si seleziona l'opzione Riferimento da una directory esterna, vengono richiesti i dettagli del server LDAP.
6. Fare clic su Salva.

   La configurazione dell'archivio utenti di CA EEM è completata.

   Nota: per ulteriori informazioni su CA EEM, consultare la *Guida in linea* di EEM.

Aggiunta di utenti e gruppi

Se CA EEM è configurato in modo da fare riferimento ad una directory esterna, non è possibile aggiungere utenti utilizzando l'interfaccia utente CA EEM. CA EEM è un'interfaccia di sola lettura del server LDAP. Per aggiornare i record utente è necessario utilizzare qualsiasi interfaccia fornita con il proprio prodotto LDAP.

Per aggiungere un nuovo record utente

1. Fare clic su Start, Programmi, CA, Embedded Entitlements Manager, UI/EEM UI.
2. Accedere utilizzando la password e il nome utente dell'amministratore CA EEM. Queste impostazioni vengono specificate nell'installazione di CA EEM. CA EEM deve essere installato separatamente e non è un'opzione di configurazione di CA SDM.
3. Fare clic sulla scheda Gestisci identità.
4. Nel riquadro di sinistra fare clic sulla scheda Utente per cercare e aggiornare i record utente esistenti.

   Nota: per gestire i gruppi CA EEM, selezionare la scheda Gruppi.
5. Fare clic sull'icona a sinistra della cartella Utenti.

   Viene visualizzato il modulo per creare un record utente.
6. Completare il modulo e fare clic su Salva.

   Il nuovo record utente CA EEM viene salvato in MDB.

Nota: la procedura necessaria per modificare un record utente esistente e gestire i record di gruppi è simile a quella illustrata. Per informazioni, vedere la *Guida in linea di CA EEM*.

Configurazione dell'accesso a CA Workflow in CA EEM

Tutti gli accessi a CA Workflow sono autenticati da CA EEM. È necessario che un utente disponga di un record utente CA EEM per accedere all'applicazione Elenco di lavoro o CA Workflow IDE. L'amministratore di CA Workflow, specificato durante la configurazione di CA SDM, dispone dell'accesso completo.

Per impostazione predefinita, l'utente viene utilizzato da CA SDM per l'integrazione di CA Workflow. Questo account utente viene impostato tramite le opzioni cawf_username e cawf_password in Gestore opzioni. È necessario accertarsi che il nome utente e la password impostati in queste opzioni siano corretti e che l'utente disponga di accesso completo alle risorse di CA Workflow all'interno di CA EEM.

CA Workflow utilizza inoltre CA EEM per limitare l'accesso a specifiche funzioni CA Workflow. Questo accesso è controllato da due classi di risorse chiamate IDE e Processo.

- La risorsa IDE è dotata di un'unica azione denominata *login*, che consente di accedere all'IDE. Per accedere all'applicazione CA Workflow IDE, è necessario disporre dell'autorizzazione.
- La risorsa Processo è dotata di un'unica azione denominata *start*, che consente di avviare un'istanza di processo. Per avviare i processi dell'applicazione Web Elenco di lavoro, è necessario disporre dell'autorizzazione.

Nota: tutti gli utenti noti a CA EEM hanno la possibilità di accedere all'applicazione Elenco di lavoro CA Workflow per visualizzare ed eseguire le attività degli elementi di lavoro. Questa autorizzazione consente solo di avviare nuove istanze dall'applicazione Elenco di lavoro. Queste classi di risorse vengono definite con l'istanza dell'applicazione CA SDM in CA EEM. Quando si accede all'interfaccia utente Web CA EEM, è necessario specificare l'istanza dell'applicazione CA SDM per visualizzare le risorse, i criteri e i gruppi trattati in questa guida.

Gli utenti che devono accedere all'IDE o avviare le istanze di processo hanno bisogno di un'autorizzazione per le risorse e le azioni precedentemente citate. La configurazione di CA SDM aggiunge due norme a CA EEM, che garantiscono l'accesso a tali risorse. Per convenienza, i criteri consentono l'accesso a due gruppi nella relativa istanza di applicazione: amministratori del flusso di lavoro e iniziatori del processo del flusso di lavoro. È sufficiente aggiungere gli utenti al gruppo di amministratori del flusso di lavoro per concedere loro il diritto di accesso all'IDE. L'aggiunta di utenti al gruppo di iniziatori del processo del flusso di lavoro consente di avviare i processi dall'applicazione Elenco di lavoro.

Per aggiungere o rimuovere gli utenti dai gruppi precedentemente menzionati

1. Accedere all'interfaccia utente Web di CA EEM
2. Nella pagina di accesso selezionare l'applicazione CA SDM e specificare il nome e la password dell'amministratore CA EEM.

3. Nella pagina principale di CA EEM selezionare Gestisci identità.
4. Selezionare il tipo di ricerca Utenti, immettere i criteri di ricerca ed eseguire la ricerca.
5. Selezionare un utente dall'elenco dei risultati.
6. Nella finestra dei dettagli dell'utente, aggiungere o rimuovere l'adesione al gruppo nella sezione Adesione gruppi applicazione.

   Nota: se questa sezione non viene visualizzata, potrebbe essere necessario premere il pulsante Dettagli utenti applicazione.
7. Al termine, premere il pulsante Salva.

   L'utente viene aggiunto o rimosso.

Assegnazione dell'elemento di lavoro CA Workflow

È possibile assegnare un ruolo di tipo Elemento di lavoro CA Workflow ad un soggetto umano o non umano. Esempi di soggetti non umani possono includere un oggetto Java personalizzato, un processo della riga di comando oppure un'altra istanza di processo di CA Workflow. Per i soggetti umani, il ruolo Elemento di lavoro è impostato su Elenco utenti globali, che rappresenta il repository utenti CA EEM. Tale repository deve essere un elenco di ID separati da punto e virgola. Ad esempio:

```
ServiceDesk; abeju01; Gruppo personale
```

assegna l'elemento di lavoro agli utenti ServiceDesk, abeju01 e agli utenti appartenenti al Gruppo personale. Ciò significa che ognuno di questi utenti può completare l'elemento di lavoro.

Nota: tutti questi utenti e gruppi devono essere noti a CA EEM. Gruppo personale rappresenta pertanto un gruppo in CA EEM e non in CA SDM.

Per assegnare in modo dinamico un gruppo di lavoro a un singolo utente, impostare l'elenco utenti Ruolo su $Utente personale.

Nota: non aggiungere le virgolette alla stringa.

Nella definizione del processo, specificare un attributo di tipo string chiamato Utente personale. Una volta creato l'elemento di lavoro, qualsiasi valore presente in Utente personale viene utilizzato per l'assegnazione dell'elemento di lavoro. Questo significa che è necessario assegnare un valore valido a Utente personale, valore che può essere un singolo nome utente oppure un elenco di nomi utente separati da punto e virgola. Questa assegnazione deve essere eseguita prima che venga utilizzata in un elemento di lavoro.

Un esempio di assegnazione di ID utente alle variabili è presente nella demo della definizione dell'ordine di un PC. La demo presuppone che l'ID utente di un record contatto di CA SDM corrisponda all'ID utente di un record utente corrispondente in CA EEM. La demo mostra come recuperare gli ID utente da CA SDM utilizzando l'interfaccia dei servizi Web. Gli ID utente possono provenire dal ticket (ad esempio l'assegnatario, l'assegnatario categoria e così via).

Per riepilogare l'impostazione dell'assegnazione di un elemento di lavoro

1. Avviare l'applicazione CA Workflow IDE.
2. Fare doppio clic sul nome della definizione di processo da modificare.

   La definizione di processo viene visualizzata nella finestra Progettazione processo.
3. Selezionare la scheda Ruoli.
4. Aggiungere o aggiornare un ruolo.
5. Selezionare Elenco utente globale dall'elenco degli attori disponibili e fare clic su Modifica.
6. Immettere un elenco di ID utente CA EEM separati da punto e virgola. È possibile utilizzare il pulsante Sfoglia per cercare e selezionare gli utenti noti a CA EEM.

Considerazioni sulla protezione

La prima volta che si installa CA SDM, il sistema è configurato per consentire il massimo accesso ai contatti che non dispongono di un tipo di accesso esplicito definito nel record di contatto. È possibile apportare ulteriori modifiche all'implementazione della protezione predefinita. Prima di consentire l'utilizzo dell'applicazione è opportuno eseguire almeno i seguenti passaggi:

1. Esaminare i tipi di accesso predefiniti per stabilirne uno che sia ragionevole per il sistema in uso.

   L'accesso predefinito è di tipo amministratore, che tuttavia non rappresenta una buona scelta per la maggior parte dei siti. Ad esempio, alcuni siti offrono accesso CA di sola lettura alla maggior parte dei membri dell'organizzazione IT. Se si imposta Utente CMDB come tipo di accesso predefinito, non è necessario impostare il tipo di accesso dei nuovi utenti, a meno che questi non necessitino di ulteriori privilegi. Analogamente, se la maggior parte degli utenti richiede il privilegio di scrivere informazioni di configurazione, è possibile scegliere Analista CMDB come tipo di accesso predefinito.
2. Assegnare i tipi di accesso ai rimanenti contatti esplicitamente.

   Se ad esempio è stato scelto Utente CMDB come tipo di accesso predefinito, è necessario modificare i record contatto per i contatti dell'analista, in modo da poter assegnare l'accesso di tipo analista.

Nota: per ulteriori informazioni, vedere la *Guida in linea*.

Autenticazione CA EEM per CA Process Automation

CA SDM e CA Process Automation comunicano tramite scambio di servizi Web su protocollo HTTP. Sebbene vengano intraprese tutte le misure possibili per trasferire il minor numero possibile di informazioni sensibili tra i prodotti, un'entità dannosa potrebbe accedere a nomi utente, password e informazioni riservate. È possibile attuare procedure apposite per proteggere la comunicazione tra server.

Per l'autenticazione CA Process Automation, considerare le seguenti raccomandazioni:

- È possibile configurare CA Process Automation per utilizzare CA EEM come server di autenticazione. CA Process Automation implementa gruppi e criteri predefiniti in CA EEM. È possibile modificare gruppi e criteri predefiniti per soddisfare le specifiche esigenze dell'organizzazione.
- L'utilizzo di CA EEM consente di evitare la necessità di passare nomi utente e password in formato testo normale per scopi di autenticazione. Se si utilizza l'opzione multi-tenancy, è necessario CA EEM per attivare più titolari in CA Process Automation.

  Nota: per ottenere la protezione dell'autenticazione in questa integrazione, non è necessario disporre di CA SDM configurato per l'utilizzo di CA EEM. Tuttavia, CA EEM è necessario per l'implementazione multi-tenancy di CA Process Automation. Per informazioni sull'implementazione dell'opzione multi-tenancy con CA Process Automation, consultare la Guida dell'utente di CA Process Automation. Nota: per informazioni sulla configurazione di CA Process Automation per usare EEM come server di autenticazione, consultare la documentazione di installazione e configurazione di CA Process Automation.
- Configurare CA Process Automation per comunicare utilizzando la comunicazione sicura su HTTPS. Gli URL HTTPS utilizzano SSL/TLS per eliminare scambi in testo normale e contemporaneamente proteggere dati riservati e altri dati sensibili dall'accesso accidentale e doloso.

  Nota: per informazioni sulla configurazione di CA Process Automation per usare HTTPS, consultare la documentazione di installazione e configurazione di CA Process Automation.

Autenticazione utente

CA SDM fornisce una soluzione di autenticazione utente che è possibile personalizzare come parte del tipo di accesso. La stessa autenticazione viene utilizzata da tutte le interfacce di CA SDM e da altri prodotti CA.

Nota: se necessario, è possibile configurare l'autenticazione utente CA SDM in un computer separato. Per ulteriori informazioni, consultare la *Guida all'implementazione*.

L'autenticazione è flessibile, consente infatti di sfruttare i vantaggi dei meccanismi di autenticazione esterna, quali la validazione utente Windows, HTTPD o l'autenticazione LDAP. È inoltre possibile scegliere tra varie opzioni interne per l'autenticazione, tra cui la password del sistema operativo, il codice PIN, l'accesso dell'utente guest oppure il divieto totale di accesso.

Modalità di autenticazione degli utenti CA SDM

CA SDM autentica gli utenti in base all'ID utente definito nel relativo record contatto. Il prodotto esegue inoltre le seguenti operazioni quando un utente richiede l'accesso al sistema:

1. Se un ID utente esterno è disponibile (dalla validazione HTTPD o Windows), <USDK> ricerca il contatto in base all'ID di accesso. Se il contatto viene trovato e il tipo di accesso a sua disposizione consente l'autenticazione esterna, l'utente può accedere al prodotto.
2. Se l'autenticazione esterna non è valida, CA SDM richiede l'ID utente e la password. Quindi, ricerca un record contatto per l'ID utente, ottiene il tipo di accesso e autentica l'utente come specificato dal tipo di accesso.

Molte installazioni considerano accettabili i tipi di accesso predefiniti che definiscono l'autenticazione dell'utente, tuttavia, in alcuni casi è necessario modificare le informazioni di autenticazione per un tipo di accesso predefinito o definire un nuovo tipo di accesso per gestire un metodo di autenticazione differente per alcuni utenti. È opportuno esaminare le impostazioni di autenticazione relative ai tipi di accesso predefiniti per stabilire se soddisfano le proprie esigenze oppure se è necessario modificarli o definirne di nuovi.

Autenticazione esterna

CA SDM consente agli utenti di accedere al sistema senza specificare un ID utente, purché siano soddisfatte le condizioni seguenti:

- Viene impostata l'autenticazione esterna per l'utente.
- L'ID utente autenticato esternamente viene associato ad un contatto della tabella dei contatti.
- Il record contatto presenta un tipo di accesso la cui definizione dell'autenticazione consente l'autenticazione esterna.

L'autenticazione non consente agli utenti di accedere al sistema nei seguenti casi:

- Un utente tenta l'accesso tramite un server non protetto.
- Un utente tenta l'accesso ma gli è stato assegnato un tipo di accesso che non consente l'autenticazione esterna.

Nessuno dei tipi di accesso predefiniti consente l'utilizzo dell'autenticazione esterna. Se si desidera utilizzare l'autenticazione esterna per gli utenti, è possibile modificare i tipi di accesso dipendente, analista e amministratore per impostare tale opzione. I requisiti di un sito e i diversi tipi di utente determinano se consentire l'autenticazione esterna. Quando viene utilizzata l'autenticazione esterna, la configurazione del server controlla l'accesso ai file e alle directory. Quando si definisce l'autenticazione per un tipo di accesso, è possibile definirne l'utilizzo come illustrato di seguito:

- Non utilizzare un'autenticazione esterna già implementata, come l'accesso utente in Windows o la validazione da parte del server HTTPD.
- Utilizzare l'autenticazione implementata e consentire o negare l'accesso in base ad essa.

Nota: se l'autenticazione esterna non è consentita, l'autenticazione dell'utente viene eseguita in base al tipo di validazione specificato.

Di seguito vengono riportati alcuni esempi di autenticazione esterna:

- Se un utente dotato di privilegi di accesso da amministratore accede ad un computer Windows, può eseguire attività amministrative senza reimmettere le informazioni di accesso.
- Se un utente dispone di validazione del server HTTPD, può accedere all'interfaccia Web senza immettere nuovamente alcuna informazione di accesso. Poiché l'accesso di tipo amministratore specifica il tipo utente Web analista, verrà fornita automaticamente l'interfaccia Web appropriata.

Nota: Per ulteriori informazioni sull'autenticazione esterna, vede lo scenario *Modalità di implementazione l'autenticazione Windows integrata per CA SDM*.

Tipi di convalida

I tipi di validazione consentono di autenticare gli utenti solo nei casi seguenti:

- Il tipo di accesso dell'utente non consente l'autenticazione esterna.
- Il tipo di accesso dell'utente consente l'autenticazione esterna ma l'utente non è stato convalidato esternamente (ad esempio, l'utente potrebbe aver tentato l'accesso attraverso un server non protetto).

In <USDK> sono disponibili le seguenti opzioni di validazione:

- **Nessun accesso**—Gli utenti di questo tipo non hanno accesso. Per accedere, l'autenticazione deve essere consentita e deve essere valida.
- **Apri**—Gli utenti di questo tipo hanno accesso senza alcuna autenticazione aggiuntiva.

- **Sistema operativo**—Gli utenti di questo tipo immettono la password del sistema operativo per effettuare l'accesso. Il sistema operativo utilizzato per la validazione è quello su cui è in esecuzione l'host della validazione utente. Questa opzione è il tipo di validazione predefinito per gli accessi di tipo amministratore, analista e dipendente.

  Nota: per ulteriori informazioni sull'host della validazione utente, consultare la *Guida all'implementazione*.

- **PIN**—Gli utenti di questo tipo ottengono l'accesso immettendo il valore corretto nel campo PIN del relativo record contatto, analogamente alla password. Quando si seleziona PIN come tipo di validazione, definire il campo PIN immettendo il nome dell'attributo del campo. PIN è il tipo di validazione predefinito per l'accesso di tipo cliente, che utilizza come PIN il valore del campo ID cliente (contact_num).

  Nota: per un elenco di nomi di attributo per l'oggetto cnt, ovvero l'oggetto definito per la tabella dei contatti, consultare la *Guida di riferimento tecnico*.

Conteggio degli utenti connessi e delle sessioni

I KPI seguenti contano il numero degli utenti con licenza univoci connessi al sistema (ad esempio, l'interfaccia utente Web di CA SDM, i servizi Web SOAP, i servizi Web REST, ecc.), indipendentemente dal numero di sessioni aperte da ciascuno di essi:

Nota: Per un utente con licenza, verificare che la casella di controllo Concesso in licenza? sia selezionata dalla pagina del tipo di accesso del contatto (accedere a Gestione protezione e ruoli, Tipo di accesso nella scheda Amministrazione e cercare il contatto).

- webConcurrentLicenseCt
- webConcurrentSOAPLicenseCt
- webConcurrentRESTLicenseCt
- webConcurrentTotalLicenseCt

I KPI seguenti contano il numero degli utenti privi di licenza univoci connessi al sistema, indipendentemente dal numero di sessioni aperte da ciascuno di essi:

- webConcurrentNonLicenseCt
- webConcurrentSOAPNonLicenseCt
- webConcurrentRESTNonLicenseCt
- webConcurrentTotalNonLicenseCt

I KPI seguenti contano il numero di sessioni univoche avviate durante l'intervallo:

- webSessionCt
- webSOAPSessionCt
- webRESTSessionCt

Per ulteriori informazioni sulla descrizione dei KPI, consultare la pagina dei dettagli relativa ai KPI (andare a Service Desk, KPI, nella scheda Amministrazione e cercare il KPI desiderato). Per ulteriori informazioni sulle modalità di conteggio dei KPI nei diversi tipi di sessione, consultare l'argomento Modalità di conteggio dei KPI nei diversi tipi di sessione (a pagina 296).

Modalità di conteggio dei KPI nei diversi tipi di sessione

Esistono diversi tipi di sessione definiti nel sistema. La tabella seguente mostra le modalità di conteggio dei KPI di queste sessioni:

Nota: Tutti i KPI predefiniti vengono installati come Non attivo. Ai fini del funzionamento di un KPI nel sistema, è necessario che sia impostato su Attivo. Accedere a Service Desk, KPI nella scheda Amministrazione e cercare il KPI non attivo. Aprire il KPI e fare clic su Attiva.

Importante: versioni multiple di un KPI con lo stesso nome non possono essere attive allo stesso tempo.

Tipo sessione	Descrizione del tipo di sessione	Calcolato dai KPI
Client Web	Sessione del browser Web	■ webSessionCt ■ webConcurrentLicenseCt ■ webConcurrentNonLicenseCt ■ webConcurrentTotalLicenseCt ■ webConcurrentTotalNonLicenseCt
Client Java	Sessione client Java	■ webConcurrentTotalLicenseCt ■ webConcurrentTotalNonLicenseCt
Servizi Web	Sessione dei servizi Web SOAP	■ webSOAPSessionCt ■ webConcurrentSOAPLicenseCt ■ webConcurrentSOAPNonLicenseCt
Utilità	Sessione dell'utilità server	■ webConcurrentTotalLicenseCt ■ webConcurrentTotalNonLicenseCt
portale	Sessione portale	■ webConcurrentTotalLicenseCt ■ webConcurrentTotalNonLicenseCt

Chat conoscenza	Sessione chat conoscenza	■ webConcurrentTotalLicenseCt ■ webConcurrentTotalNonLicenseCt
Server di posta elettronica	Sessione del server di posta elettronica	■ webConcurrentTotalLicenseCt ■ webConcurrentTotalNonLicenseCt
Applicazione personalizzata	Sessione applicazione personalizzata	■ webConcurrentTotalLicenseCt ■ webConcurrentTotalNonLicenseCt
Client PDA	Sessione del client PDA	■ webSessionCt ■ webConcurrentLicenseCt ■ webConcurrentNonLicenseCt ■ webConcurrentTotalLicenseCt ■ webConcurrentTotalNonLicenseCt
Client REST	Sessione dei servizi Web REST	■ webRESTSessionCt ■ webConcurrentRESTLicenseCt ■ webConcurrentRESTNonLicenseCt ■ webConcurrentTotalLicenseCt ■ webConcurrentTotalNonLicenseCt

Esempio: KPI che calcolano i conteggi dell'utente

Un utente finale con licenza (con la casella di controllo Concesso in licenza? selezionata) e due utenti finali privi di licenza sono connessi all'interfaccia self-service Web e stanno revisionando alcuni annunci.

Nello stesso tempo cinque analisti con licenza (con la casella di controllo Concesso in licenza? selezionata) sono connessi all'interfaccia degli analisti e stanno lavorando su alcuni Incidenti. Uno degli analisti si connette anche all'Interfaccia dei servizi Web SOAP.

- Il KPI webConcurrentLicenseCt riporta un conteggio pari a sei, che indica che attualmente sono utilizzate sei licenze, senza tener conto del numero di interfacce che ciascun utente sta utilizzando.
- Il KPI webConcurrentNonLicenseCt riporta un conteggio pari a due, che indica che due utenti privi di licenza sono connessi al sistema, senza tener conto del numero di interfacce che ciascun utente sta utilizzando.
- Il KPI webSessionCt riporta un conteggio pari a otto, che indica che in totale sono otto gli utenti connessi all'interfaccia Web di CA SDM.
- Il KPI webSOAPSessionCt riporta un conteggio pari a uno, che indica che un solo utente è connesso all'interfaccia dei servizi Web SOAP.

(Valido solo per la configurazione della disponibilità avanzata) Esempio: KPI che calcolano i conteggi utente da nodi differenti

Un analista con licenza accede all'interfaccia degli analisti dal server in background e lavora sugli Incidenti. Lo stesso analista accede all'interfaccia degli analisti dal server applicazioni. Il KPI webConcurrentLicenseCt riporta un conteggio pari a uno, che indica che attualmente viene utilizzata una licenza, senza tener conto del numero di nodi o server da cui l'utente ha eseguito l'accesso.

Registri interni

È possibile definire se un determinato tipo di accesso consente la visualizzazione dei registri interni. In tal caso, in ognuna delle finestre Registro attività, i contatti avranno a disposizione una casella di controllo chiamata Contrassegna come interna. Quando le attività sono contrassegnate come interne, solo i contatti con un tipo di accesso che consente la visualizzazione dei registri interni vedranno l'attività o riceveranno la relativa notifica.

Integrazione di CA SDM

Il tipo di accesso identifica anche il tipo di utente che adotta questo tipo di accesso quando utilizza altri prodotti CA con CA SDM. Quando un contatto con questo tipo di accesso utilizza l'altro prodotto, i diritti di accesso per tale prodotto vengono determinati dai valori specificati per il tipo di accesso.

Associazioni delle partizioni dati

Le partizioni dati possono essere assegnate a singoli contatti, ma il metodo preferito consiste nell'assegnazione in base al tipo di accesso. Dopo l'associazione delle partizioni dati a tipi di accesso differenti, è possibile associare un contatto a un tipo di accesso specifico e definirne la partizione dati. Il tipo di accesso dispone di un'opzione specifica per ignorare la partizione dati del contatto.

Per associare una partizione dati ad un tipo di accesso, è necessario impostare partizioni dati che siano significative per il sito, quindi selezionare una delle partizioni dati quando si definisce o si modifica un tipo di accesso.

Importante. altre impostazioni di protezione di CA SDM potrebbero avere la precedenza su quelle presenti nelle partizioni dati.

Configurazione della partizione dati

Una partizione dati è un sottoinsieme di un database di CA SDM che controlla l'accesso dell'utente ai ticket e ad altri record di dati in base al relativo contenuto.

Ad esempio, è possibile limitare a un utente la visualizzazione del database relativamente ai soli elementi della configurazione assegnati all'organizzazione dell'utente. È inoltre possibile consentire all'utente di aggiornare solo i ticket assegnati e concedere l'accesso in sola lettura agli altri elementi della configurazione.

Una partizione dati è costituita da una serie di vincoli. I vincoli della partizione dati identificano la tabella controllata dalla partizione dati e il tipo di vincolo. I tipi di vincolo specificano le operazioni che l'utente può eseguire nella partizione dati, ad esempio operazioni di creazione, eliminazione, aggiornamento, visualizzazione e così via. Dopo aver assegnato una partizione dati ad un tipo di accesso, a sua volta assegnato ad un record contatto dell'utente, sono i vincoli e i tipi di vincolo a controllare l'accesso dell'utente ai record della tabella di database di CA SDM.

Inoltre, è possibile visualizzare i vincoli indipendenti dalla partizione dati che li utilizza. Ad esempio, si desidera visualizzare tutti i vincoli di una specifica tabella, indipendentemente dalla partizione dati.

Verifica dei prerequisiti

Prima di configurare la partizione dati, verificare i prerequisiti seguenti:

- Policy e struttura di protezione dei dati (a pagina 299)
- Configurazione delle partizioni dati (a pagina 300)
- Specifiche del vincolo (a pagina 301)

Policy e struttura di protezione dei dati

La pianificazione della protezione dei dati implica l'imposizione di restrizioni per l'accesso a una porzione specifica del database. È possibile imporre queste restrizioni su contatti individuali o mediante ruoli o tipi di accesso:

Ruoli

Definisce la funzionalità a cui gli utenti nel ruolo possono accedere. È possibile assegnare uno o più ruoli al record di un contatto individuale o a un tipo di accesso per definire l'accesso funzionale per tutti i tipi di accesso associati a contatti.

Tipo di accesso

Definisce come i contatti vengono autenticati quando accedono all'interfaccia Web. Ad esempio, un tipo di accesso decide se i contatti possono modificare i moduli Web o lo schema del database mediante Web Screen Painter e quali ruoli sono disponibili per i contatti.

Come amministratore Service Desk, è possibile modificare i tipi di accesso predefiniti ed è possibile crearne di nuovi. È possibile imporre la restrizione agli utenti individuali o a un gruppo di utenti mediante l'opzione Ruoli.

Identificare quanto segue:

- Gli oggetti e il tipo di restrizioni che si desidera imporre su questi oggetti.
- Gli utenti o i ruoli a cui viene applicata la partizione dati. È possibile applicare le partizioni dati ai contatti direttamente, ma il metodo preferito è quello di assegnare le partizioni in base al ruolo e di assegnare tale ruolo a tutti i contatti direttamente o mediante il tipo di accesso.

Specifiche di configurazione delle partizioni dati

È possibile definire un numero illimitato di partizioni dati. Ogni partizione dati è costituita da una serie di vincoli e convalide in ogni tabella di database limitata dalla partizione dati. Per ogni tabella della partizione dati, è possibile specificare autorizzazioni indipendenti per visualizzare, aggiornare, creare o eliminare i record utilizzando i criteri specificati in un formato simile a una clausola SQL WHERE. È possibile basare la limitazione su qualunque attributo del record a cui si ha avuto accesso, insieme a qualsiasi altro tipo di dati del record contatto dell'utente. Questo consente una notevole flessibilità durante il processo di definizione delle partizioni dati. Ad esempio, l'uso del campo Vendor della tabella Contatto, consente l'applicazione di limitazioni della partizione dati ai vendor ai quali è consentito l'accesso diretto a CA SDM.

per motivi di prestazioni, CA SDM non consente la presenza di un'unione cartesiana in un vincolo della partizione dati. Un'unione cartesiana deriva da un vincolo contenente un operatore “OR” che limita tutte le tabelle unite in entrambi i lati dell'operatore OR. Per garantire che il vincolo della partizione dati non produca un'unione cartesiana, immettere il comando seguente:

Windows

```
bop_cmd -f $NX_ROOT\bopcfg\interp\bop_diag.frg "check_queries()"
```

UNIX

```
bop_cmd -f $NX_ROOT/bopcfg/interp/bop_diag.frg "check_queries()"
```

Importante. Le partizioni dati contrassegnate da questo programma devono essere aggiornate nel modo appropriato.

Specifiche del vincolo

I vincoli e i test di validazione vengono specificati in Majic, utilizzando il metalinguaggio di definizione degli oggetti.

Nota: per ulteriori informazioni, consultare la *Guida di riferimento tecnico*.

I vincoli definiti in Majic sono molto simili alla clausola SQL WHERE ma con le eccezioni seguenti:

- I nomi di attributo nel vincolo sono nomi di attributo dell'oggetto e non nomi di attributo del database tratti dallo schema.
- È possibile fare riferimento al valore di un attributo nel record contatto per l'utente-collegato con un nome specificato nel formato seguente, dove *att_name* è il nome Majic dell'attributo desiderato:

  ```
  @root.nome_att
  ```

  Ad esempio, se si specifica @root.location si fa riferimento all'ID dell'ubicazione del contatto corrente.

  Le unioni vengono specificate nel formato seguente, in cui *foreign-key* è il nome Majic dell'attributo nella tabella per cui si sta creando il vincolo partizione dati e *attribute-in-referenced-table* è il nome Majic dell'attributo nella tabella unita:

  ```
  foreign-key.attribute-in-referenced-table
  ```

  Per fare ad esempio riferimento al vendor addetto alla gestione dell'asset associato a un report Incidente, specificare:

  ```
  resource.vendor_repair
  ```

  Questo tipo di specifica è ricorsivo. Ad esempio è possibile fare riferimento al nome del vendor specificando il nome seguente:

  ```
  resource.vendor_repair.name
  ```

La seguente tabella contiene esempi di vincoli validi da utilizzare per la tabella Change_Request utilizzata per memorizzare le informazioni sugli Ordini di cambiamento:

Tipo vincolo	Codice e descrizione
Visualizza	assignee.organization = @root.organization Indica che l'utente può visualizzare unicamente gli Ordini di cambiamento in cui l'organizzazione dell'assegnatario corrisponde all'organizzazione dell'utente.

Aggiornamento preliminare	requestor = @root.id Indica che l'utente può aggiornare unicamente gli Ordini di cambiamento di cui è il chiamante o il richiedente.

Non è tuttavia possibile scrivere vincoli che utilizzano unioni in entrambi i lati dell'espressione, come illustrato nell'esempio seguente:

```
assignee.org = requestor.org
```

Visualizzazione delle tabelle controllate da partizioni dati

Una tabella controllata è un elenco di tabelle su cui un amministratore Service Desk può imporre limitazioni mediante le partizioni dati. Queste tabelle danno un'idea degli oggetti e delle tabelle per i quali è possibile limitare l'accesso utente.

Nota: non è possibile aggiungere o eliminare tabelle controllate o modificarne i nomi oggetto.

Procedere come descritto di seguito:

1. Selezionare Gestione protezione e ruoli, Partizioni dati, Tabelle controllate da partizioni dati nella scheda Amministrazione.

   Compare l'elenco delle tabelle controllate.

2. (Facoltativo) Fare clic su Mostra filtro e compilare uno o più campi di ricerca.
3. Selezionare il nome della tabella da visualizzare.

   Viene visualizzata la pagina Dettagli tabella controllata dalla partizione dati.

Creazione di un vincolo partizione dati

I vincoli di partizione dati limitano l'accesso ai record del database per gli utenti assegnati alla partizione dati.

Procedere come descritto di seguito:

1. Selezionare Gestione protezione e ruoli, Partizioni dati, Vincoli partizione dati nella scheda Amministrazione.

   Viene visualizzata la pagina Elenco Vincoli partizione dati.

2. Fare clic su Crea Nuovo.

   Viene visualizzata la pagina Crea Nuovo vincolo partizione dati.

3. Completare i campi del vincolo partizione dati (a pagina 304), secondo necessità.
4. Completare le informazioni nelle schede, secondo necessità:

   Vincolo

   Consente di specificare i criteri che controllano i record della tabella che possono essere visualizzati, creati, aggiornati o eliminati da un utente assegnato alla partizione dati. Ad esempio, è possibile specificare che gli utenti possono unicamente aggiornare le Issue di cui sono assegnatari. Quando un utente nella partizione dati richiede un record non soddisfa la condizione, tale record sarà di sola lettura.

   Limite: 4000 byte

   Conversione SQL

   Consente di visualizzare la definizione di vincolo in formato SQL. La condizione immessa nella scheda Vincolo viene convalidata e viene creata la clausola SQL WHERE, visualizzata nella scheda Conversione SQL per verifica.

5. Fare clic su Salva.

   Il vincolo viene salvato e aggiunto alla partizione dati.

Esempio: creazione di un vincolo di partizione dati per le assegnazioni CAB

È possibile creare un vincolo di partizione dati che consenta agli utenti di aggiornare solo gli Ordini di cambiamento assegnati a un CAB a cui appartiene l'utente che ha effettuato l'accesso.

Per creare un vincolo di partizione dati per le assegnazioni degli Ordini di cambiamento al gruppo CAB, assegnare i seguenti valori di vincolo per una tabella controllata Change_Request in una partizione dati:

- Tipo vincolo: Aggiornamento preliminare
- Descrizione del vincolo: cab.[group]group_list.member IN (@root.id)

L'utente che ha effettuato l'accesso può aggiornare solo gli Ordini di cambiamento assegnati a un gruppo CAB a cui l'utente appartiene.

Vedi anche

Campi Vincoli partizione dati (a pagina 304)
Definizione dei vincoli (a pagina 306)

Campi Vincoli partizione dati

Completare i campi seguenti per aggiungere o modificare i campi del vincolo partizione dati:

Nome partizione dati

Specifica il nome della partizione dati per cui viene definito il vincolo.

Nome tabella

Specifica la tabella del database controllata dal vincolo.

Tipo vincolo

Definisce il tipo di vincolo che viene definito. Per ciascuna tabella in una partizione dati sono disponibili sei tipi di vincoli,

Crea

Specifica i criteri che devono essere soddisfatti prima di creare un record. Quando un utente nella partizione dati tenta di creare un record che non soddisfa la condizione di creazione, CA SDM visualizza un messaggio di errore associato al vincolo e non salva il record.

Impostazioni predefinite

Specifica una o più istruzioni di assegnazione, separate da punto e virgola, che definiscono i valori da assegnare ai campi vuoti in un nuovo record al momento della memorizzazione del record. La sintassi di ogni istruzione di assegnazione è la seguente, in cui *nome_att* è il nome di un attributo Majic del record e *valore* può essere un valore intero, una stringa tra virgolette o un riferimento in formato @root.*nome_att* a un attributo Majic nel record contatto dell'utente corrente:

```
nome_att=valore
```

Per le tabelle aggiornate in base ai ticket, i valori predefiniti vengono inseriti nel record quando questo viene visualizzato e i valori vengono mostrati durante la visualizzazione iniziale di un nuovo record. È possibile assegnare un valore predefinito a un campo di riferimento (uno SREL Majic) codificandolo nel formato di un ID persistente. Un ID persistente è un nome di oggetto seguito da un carattere due punti (:) e da un valore numerico intero per l'ID. Ad esempio, è possibile impostare un valore predefinito per la categoria includendo quanto segue nella specifica delle impostazioni predefinite, in cui PCAT è la destinazione dello SREL (come mostrato nel file Majic) e 12345 è il numero di ID della categoria desiderata:

```
category='PCAT:12345'
```

Per elencare gli ID persistenti di un oggetto, utilizzare il comando nel formato seguente:

```
bop_odump domsrvr pcat "" sym
```

Elimina

Specifica i criteri che devono essere soddisfatti per eliminare un record. Quando un utente nella partizione dati tenta di eliminare un record che non soddisfa la condizione di eliminazione, CA SDM visualizza un messaggio di errore associato al vincolo e non elimina il record.

Aggiornamento preliminare

Specifica i record della tabella controllata che un utente può aggiornare nella partizione dati. Quando un utente nella partizione dati richiede un record che non soddisfa la condizione di aggiornamento preliminare, CA SDM imposta il record in sola lettura e visualizza il messaggio di errore definito con il vincolo.

Aggiorna

Specifica i criteri che devono essere soddisfatti quando un record viene salvato. Quando un utente nella partizione dati tenta di salvare un record che non soddisfa la condizione di aggiornamento, CA SDM visualizza un messaggio di errore associato al vincolo e non salva il record.

Visualizza

Specifica i record della tabella controllata che un utente può visualizzare nella partizione dati. Questo vincolo viene automaticamente applicato a tutti gli elenchi selezionati da un utente in questa partizione dati, in aggiunta a qualsiasi criterio di selezione specificato esplicitamente dall'utente.

Questo vincolo può includere unioni in altre tabelle e riferimenti nel formato @root.*nome_att* agli attributi Majic nel record contatto dell'utente corrente o collegato. Esempi di valori validi sono:

```
requestor.organization = @root.organization
```

```
requestor.organization.name = 'MIS'
```

```
assignee = @root.id
```

```
assignee.organization = @root.organization
```

Nota: i tipi di vincolo Crea, Elimina, Agg prelim e Aggiorna supportano ora le unioni ad altre tabelle. Possono inoltre includere riferimenti nel formato @root.attribute ad attributi del record contatto dell'utente corrente.

Stato record

Indica se il vincolo è attivo o inattivo.

Messaggio di errore

Specifica il messaggio restituito all'utente se i criteri del vincolo non vengono soddisfatti. Ad esempio, "È possibile solo aggiornare le Issue assegnate" o "È possibile solo creare Issue per la propria organizzazione" o "È possibile aggiornare il record di contatto ma non modificare la partizione dati".

Definizione dei vincoli

Specificare la condizione in formato Majic (metalinguaggio utilizzato per definire gli oggetti di CA SDM).

Se il Tipo vincolo è Visualizza, la condizione può includere unioni ad altre tabelle e riferimenti in formato @root.att_name ad attributi Majic nel record di contatto per l'utente collegato. Gli altri tipi non possono includere unioni ad altre tabelle ma solo riferimenti in formato @root.att_name ad attributi Majic nel record di contatto per l'utente collegato.

Se il Tipo vincolo è Predefinito, è possibile specificare una o più istruzioni di assegnazione, separate da punto e virgola, che indicano i valori da assegnare ai campi vuoti in un nuovo record nel momento in cui questo viene memorizzato. La sintassi di ciascuna istruzione di assegnazione è:

```
att_name=value
```

dove att_name indica il nome di un attributo Majic nel record e value può essere costituito da un valore intero, una stringa tra virgolette, o un riferimento in formato @root.att_name a un attributo Majic nel record di contatto per l'utente collegato. Il modo in cui CA SDM utilizza i valori predefiniti varia a seconda della tabella interessata.

Per le tabelle aggiornate da CA SDM, ad esempio Questioni, i valori predefiniti vengono posizionati nel record nel momento in cui questo viene visualizzato e sono indicati nella visualizzazione iniziale di un nuovo record. È possibile assegnare un valore predefinito a un campo di riferimento (un SREL Majic) codificandolo nel formato di un ID persistente, ossia un nome tabella seguito da due punti e un ID intero. Ad esempio, è possibile impostare un valore predefinito per la categoria immettendo la stringa seguente nella specifica Predefinito:

```
category='PCAT:12345'
```

dove 'PCAT' indica la destinazione SREL, riportata nel file Majic, e 12345 rappresenta il numero ID della categoria desiderata. È possibile elencare gli ID persistenti per una tabella con un comando di tipo:

```
bop_odump domsrvr pcat "" sym
```

Creazione di una partizione dati

Una partizione dati è un sottoinsieme di un database di CA SDM che controlla l'accesso dell'utente ai ticket e ad altri record di dati in base al relativo contenuto.

Procedere come descritto di seguito:

1. Selezionare Gestione protezione e ruoli, Partizioni dati, Elenco partizioni dati nella scheda Amministrazione.

   Viene aperta la pagina Elenco partizioni dati.

2. Fare clic su Crea Nuovo.

   Viene visualizzata la pagina Crea Nuova partizione dati.

3. Compilare i campi in modo appropriato:

   Partizione dati

   Specifica un identificatore univoco per la partizione dati.

   Stato record

   Indica se la partizione è attiva o inattiva.

4. Fare clic su Salva.
5. Fare clic su Nuovo vincolo e associare le definizioni di vincolo alla partizione.
6. Fare clic su Salva.

   La partizione dati viene salvata con il vincolo partizione dati.

Vedi anche

Creazione di un vincolo partizione dati (a pagina 303)

Creazione di un tipo di accesso

I tipi di accesso definiscono tutti gli aspetti della protezione. Sono inclusi vari tipi predefiniti di accesso ed è possibile modificarli o definirne di nuovi. Ogni tipo di accesso per un utente controlla i seguenti aspetti del comportamento di sistema:

- Il modo in cui CA SDM esegue l'autenticazione Web quando l'utente esegue l'accesso.
- Il livello di accesso per l'utente.
- La possibilità da parte dell'utente di modificare i moduli Web o lo schema del database mediante Web Screen Painter.
- I ruoli disponibili per l'utente.

Procedere come descritto di seguito:

1. Selezionare Gestione protezione e ruoli, Tipi di accesso nella scheda Amministrazione.

   Viene visualizzata la pagina Elenco Tipi accesso.

   Valore predefinito: 15

2. Fare clic su Crea Nuovo e completare i campi del tipo di accesso (a pagina 308), secondo necessità, nella pagina Crea nuovo tipo di accesso.

3. Utilizzare le schede per completare le attività seguenti:

   - Configurazione dell'autenticazione Web per un tipo di accesso (a pagina 309)
   - Assegnazione di autorizzazioni Web Screen Painter a un tipo di accesso (a pagina 310)
   - Assegnazione di ruoli a un tipo di accesso (a pagina 311)

4. Fare clic su Salva.

   Viene creato il tipo di accesso.

Campi Tipo di accesso

Nelle pagine Crea tipo di accesso, Dettagli tipo accesso e Aggiorna tipo accesso compaiono i seguenti campi.

Simbolo

Specifica un identificatore univoco per il tipo di accesso.

Predefinito?

Indica se il tipo di accesso è quello predefinito associato ai contatti.

Stato record

Specifica se il tipo di accesso è attivo o non attivo.

Descrizione

Descrive il tipo di accesso. Tale campo è utile per identificarne meglio le caratteristiche del tipo di accesso.

Ricezione notifica interna

Determina se i contatti associati al tipo di accesso ricevono una notifica interna sulle attività relative ai ticket.

Livello di accesso

Determina i tipi di accesso che un utente può concedere a un altro utente. È possibile assegnare un tipo di accesso al record di contatto di un altro utente solo se il livello di accesso del tipo che si desidera assegnare è uguale o inferiore al livello di concessione di cui si dispone per il proprio tipo di accesso. I livelli sono classificati come segue:

- Amministrazione (il più alto)
- Analista
- Cliente/Dipendente
- Nessuno (il più basso)

Concesso in licenza?

Determina se questo contatto è un tipo di accesso concesso in licenza. I contatti ai quali è assegnato un tipo di accesso non concesso in licenza possono visualizzare o aggiornare solo i dati personali.

Nota: il KPI conteggia il numero di utilizzi utente simultanei dal sistema (ad esempio, interfaccia utente Web CA SDM, servizi Web SOAP, servizi Web REST, ecc). Ad esempio, il KPI webConcurrentLicenseCt conta il numero massimo di utenti univoci (con l'opzione Concesso in licenza? selezionata) che hanno effettuato l'accesso all'interfaccia utente Web CA SDM durante l'intervallo. Per maggiori informazioni sui conteggi degli utenti collegati e licenziatari, consultare la *Guida all'amministrazione*

Configurazione dell'autenticazione Web per un tipo di accesso

È possibile configurare l'autenticazione Web e il tipo di validazione per specificare il modo in cui i ruoli assegnati a questo tipo di accesso vengono autenticati quando gli utenti tentano di accedere ai prodotti CA. Completare i campi seguenti nella scheda Autenticazione Web.

Consenti autenticazione esterna

Selezionare questa casella di controllo se si desidera che i contatti vengano autenticati esternamente, ad esempio dal server HTTPD o dal sistema operativo. Se si seleziona questa opzione, gli utenti con questo tipo di accesso vengono convalidati dal metodo esterno appropriato some configurato durante l'installazione. Verifica che la convalida esterna sia stata eseguita effettivamente (ad esempio, verifica se l'utente ha tentato di accedere mediante un server non protetto) e che l'utente sia definito come un contatto valido nel sistema attraverso il proprio ID di accesso. Quindi, utilizza il tipo di accesso per determinare l'interfaccia corretta da utilizzare.

Tipo convalida

Definisce il modo in cui gli utenti vengono autenticati quando un'autorizzazione esterna non è permessa o non riesce (ad esempio, se l'utente tenta di effettuare l'accesso mediante un server non sicuro). Le opzioni disponibili sono:

Nessun accesso

Nega l'accesso ai prodotti CA, a meno che l'autenticazione esterna non sia consentita e valida.

Aperto

L'accesso ai prodotti CA è sempre consentito, senza che sia necessaria un'autenticazione aggiuntiva.

OS

L'accesso ai prodotti CA è consentito attraverso il nome utente e la password del sistema operativo.

PIN/Numero PIN

Gli utenti di questo tipo possono accedere solo se immettono il valore corretto nel campo PIN del loro record contatto. Se si seleziona l'opzione PIN, è possibile scegliere quale campo del record contatto memorizza il PIN immettendo il nome attributo del campo nella casella di modifica Campo PIN.

CA EEM

L'accesso ai prodotti CA è consentito attraverso CA EEM. Questa opzione è disponibile solo se CA SDM è integrato con CA EEM.

Assegnazione di autorizzazioni Web Screen Painter a un tipo di accesso

L'utilità Web Screen Painter (WSP) consente agli utenti di CA SDM di creare e pubblicare moduli Web e schemi. La scheda Screen Painter Web controlla anche l'accesso al database per le sessioni di anteprima di Screen Painter Web. Per informazioni dettagliate su WSP, consultare la *Guida in linea di Screen Painter Web*.

Selezionare le autorizzazioni che si desidera concedere per un tipo di accesso nella scheda Screen Painter Web.

Modifica moduli

Consente agli utenti di modificare i moduli esistenti senza che i cambiamenti siano disponibili per tutti gli utenti.

Modifica schema

Consente agli utenti di modificare uno schema esistente senza che i cambiamenti siano disponibili per tutti gli utenti.

Pubblica moduli

Consente agli utenti di rendere disponibili i moduli modificati a tutti gli utenti.

Pubblica schema

Consente agli utenti di rendere disponibili gli schemi modificati a tutti gli utenti.

È possibile aggiornare il database nella sessione di anteprima

Consente agli utenti di apportare cambiamenti al database durante una sessione di anteprima. Per impostazione predefinita, i cambiamenti al database non sono consentiti durante una sessione di anteprima.

Assegnazione di ruoli a un tipo di accesso

L'assegnazione di ruoli a un tipo di accesso limita l'accesso alle aree funzionali per i contatti assegnati ai ruoli.

Procedere come descritto di seguito:

1. Selezionare i ruoli riportati di seguito per il tipo di accesso:

   Ruolo di reporting

   Definisce l'accesso al reporting per questo tipo.

   Ruolo API del servizio Web REST

   Definisce l'accesso ai servizi Web REST per questo tipo.

   Ruolo API del servizio Web SOAP

   Definisce l'accesso ai servizi Web SOAP per questo tipo.

   Ruolo utilità riga di comando

   Definisce l'accesso alle utilità della riga di comando per questo tipo.

2. Fare clic su Aggiorna ruoli.

   Viene visualizzata la pagina Ricerca Ruolo.

3. Immettere i criteri di ricerca per restringere l'elenco ai ruoli desiderati, quindi fare clic su Cerca.

   Viene visualizzata la pagina Ruoli assegnati Aggiornamento, che elenca i ruoli corrispondenti ai criteri di ricerca.

4. Selezionare i ruoli da assegnare a questo tipo di accesso dall'elenco di sinistra. Per selezionare più elementi, tenere premuto il tasto Ctrl mentre si fa clic con il pulsante sinistro del mouse.

5. Fare clic sulle frecce direzionali a destra doppie dopo avere selezionato tutti i ruoli desiderati.

   I ruoli selezionati vengono spostati nell'elenco di destra Ruoli assegnati.

6. Fare clic su OK.

   Viene visualizzata la pagina Dettagli tipo accesso, in cui i ruoli assegnati sono elencati nella scheda Ruoli.

7. Fare clic su Salva.

   Viene visualizzata la pagina Dettagli tipo accesso, in cui un messaggio conferma che i cambiamenti sono stati salvati.

8. Selezionare il ruolo che deve essere quello predefinito per questo tipo di accesso quando si effettua l'accesso, quindi fare clic su Imposta ruolo predefinito.

   La selezione del ruolo predefinito viene salvata.

Aggiunta della partizione dati a un ruolo

Passare al ruolo a cui la partizione dati è stata collegata. Il ruolo ha accesso solamente alla partizione dati a cui è assegnato.

Procedere come descritto di seguito:

1. Selezionare Gestione protezione e ruoli, Gestione ruoli, Elenco Ruoli, nella scheda Amministrazione.

   Viene visualizzata la pagina Elenco ruoli.

2. Selezionare un ruolo e fare clic su Modifica.
3. Accedere alla scheda Autorizzazione e fare clic su Nome partizione dati.
4. Cercare e selezionare il nome della partizione dati dall'elenco partizione dati.
5. Nella scheda Autorizzazione, selezionare Sovrascrivere la partizione dati del contatto?. Quando l'opzione Sovrascrivi partizione dati del contatto è selezionata, viene imposta la partizione dati del ruolo altrimenti viene imposta quella del contatto.
6. Fare clic su Salva.

Verifica dei vincoli di partizione dati

La verifica dei vincoli di partizione dati consente di assicurare che la restrizione creata venga imposta sui contatti in modo appropriato. Tentare di visualizzare o modificare i record di dati ai quali il vincolo della partizione dati dovrebbe limitare l'accesso.

Procedere come descritto di seguito:

1. Accedere a CA SDM utilizzando il contatto per cui sono state imposte le restrizioni della partizione dati.
2. Tentare di eseguire l'accesso ai dati degli oggetti su cui sono imposti i vincoli delle partizioni dati.

   Se le restrizioni funzionano secondo le impostazioni, la partizione dati è stata creata e applicata correttamente.

Configurazione di vincoli di partizione dati di Gestione della conoscenza per autorizzazioni in base al ruolo

Le partizioni di dati sono attivate per impostazione predefinita in Gestione della conoscenza per consentire di utilizzare autorizzazioni in base a ruolo e gruppo. Se si esegue l'aggiornamento da una versione precedente, i vincoli delle partizioni di dati vengono aggiornati dallo strumento di migrazione.

Se si utilizzano vincoli di partizioni di dati personalizzati per gestire autorizzazioni della conoscenza in una versione precedente, è necessario aggiornare manualmente i vincoli per le tabelle O_INDEXES e SKELETONS. È possibile visualizzare i vincoli delle partizioni di dati predefiniti e applicarvi eventuali modifiche in base a quanto richiesto dall'ambiente in uso.

Procedere come descritto di seguito:

1. Selezionare Gestione protezione e ruoli, Partizioni dati, Vincoli partizione dati nella scheda Amministrazione.

   Viene visualizzata la pagina Elenco Vincoli partizione dati.

2. Fare clic su Mostra filtro ed eseguire una ricerca utilizzando i seguenti criteri di ricerca:

   - Immettere **Analista Service Desk** nella ricerca Partizione dati.
   - **O_INDEXES** nella ricerca Tabella.

3. Modificare il tipo di vincolo Visualizzazione modificando la scheda Vincolo sostituendo "READ_PGROUP in @root.pgroups" come indicato di seguito:

   ```
   READ_PGROUP in @root.pgroups
   ```

   ```
   READ_PGROUP.[pgroup]contained_roles.role IN @root.id
   ```

4. Salvare il vincolo.

5. Modificare i tipi di vincolo Cancella e Aggiornamento preliminare modificando la scheda Vincolo sostituendo "WRITE_PGROUP in @root.pgroups" come indicato di seguito:

   ```
   WRITE_PGROUP in @root.pgroups OR WRITE_PGROUP.[pgroup]contained_roles.role IN
   @root.role
   ```

6. Salvare i vincoli.

7. Ripetere la procedura per aggiornare i vincoli Visualizza, Elimina e Agg prelim nella tabella SKELETONS nella partizione di dati.

   I vincoli della partizione di dati vengono aggiornati.

Indagini

Le indagini cliente consentono agli amministratori di CA SDM di raccogliere in modo sistematico e analizzare i commenti del cliente in merito alle prestazioni del service desk. È possibile personalizzare le indagini in base esigenze alle specifiche del proprio sito.

Configurazione del sistema per le indagini

Prima di poter utilizzare le indagini, è necessario configurare il sistema nel modo appropriato, attraverso le due procedure seguenti:

1. Installare e configurare l'interfaccia Web CA SDM. Quando un utente accede all'URL per un'indagine, l'interfaccia Web specifica il formato dell'indagine e inserisce le relative informazioni. Per ulteriori informazioni, consultare la *Guida all'implementazione*.
2. Utilizzando Gestore opzioni, configurare e installare l'opzione web_cgi_url per specificare l'ubicazione del motore Web CA SDM. Per informazioni dettagliate, consultare il capitolo "Controllo del comportamento del sistema" e vedere la *Guida in linea*.

Preparazione di un'indagine

Preparare le indagini utilizzando Elenco indagini cliente, una tipica finestra di elenco. Ad esempio, è possibile utilizzare questa finestra per visualizzare tutte le indagini o un sottoinsieme in base ai criteri specificati; è possibile creare nuove indagini, visualizzare i dettagli di una specifica indagine ed eseguire segnalazioni sulle indagini presenti nell'elenco.

Per ogni indagine è possibile definire quanto segue:

- Un nome che è possibile utilizzare a scopo di ricerca e di segnalazione.
- Un'introduzione che è possibile utilizzare per spiegare ai clienti lo scopo dell'indagine.
- Un elenco di domande per il cliente, ognuna delle quali include un set di possibili risposte.
- Un'area facoltativa in cui l'utente può immettere liberamente dei commenti.
- Un messaggio di completamento da visualizzare dopo l'invio dell'indagine da parte dell'utente.

Nota: per ulteriori informazioni su come creare indagini, vedere la *Guida in linea*.

Definizione di notifiche di indagine.

La scheda Indagine della pagina Aggiorna notifica attività consente di definire una notifica di indagine per una notifica attività. All'attivazione della notifica attività selezionata, il contatto che ha avviato l'attività riceve la notifica di indagine. Un registro attività viene generato sia quando una notifica indagine viene inviata sia quando una notifica indagine torna indietro da un cliente.

Per impostare una notifica di indagine

1. Nella scheda Amministrazione, accedere a Notifiche, Notifiche attività.

   Viene visualizzato l'elenco Notifiche attività.

2. Selezionare la notifica attività desiderata.

   Viene visualizzata la pagina dei dettagli.

3. Fare clic sul pulsante Modifica.

   Viene visualizzata la pagina Aggiorna notifica attività.

4. Modificare i campi in modo appropriato.
5. Selezionare un tipo di oggetto dall'elenco a discesa.
6. Fare clic sulla scheda Indagine.

   In questa scheda sono disponibili i seguenti campi:

   Invia l'indagine

   Questa casella di controllo consente di attivare o disattivare l'indagine. Se selezionata, l'indagine viene inviata al contatto all'attivazione dell'attività di notifica selezionata.

   Indagine predefinita

   Specificare un'indagine predefinita utilizzando l'icona di ricerca o specificarne una propria nella casella di testo.

   Metodo di notifica

   Scegliere *uno* dei seguenti metodi di modifica:

   - Posta elettronica
   - Notifica
   - Posta elettronica cercapersone

Titolo del messaggio indagine

Immettere il titolo dell'indagine.

Testo del messaggio indagine

Immettere un messaggio per il contatto. Quando un contatto riceve la notifica di un'indagine, il corpo del messaggio include automaticamente un URL al quale il cliente può accedere direttamente dal proprio browser Web per trovare e completare il modulo di indagine.

7. Salvare la notifica attività.

   All'attivazione della notifica attività selezionata, il contatto che ha avviato l'attività riceve la notifica di indagine.

Segnalazioni per le indagini

In CA SDM è possibile creare normalmente segnalazioni per le indagini dalla scheda Amministrazione del client Web. Ad esempio, dal menu File della finestra Elenco indagini cliente è possibile scegliere Rapporti e quindi scegliere un rapporto Riepilogo o Dettagli. Dalle varie finestre dei dettagli è anche possibile scegliere Stampa modulo per stampare i dati del modulo per le indagini, per le questioni e per le risposte.

È inoltre possibile generare i rapporti in base ai dati delle indagini presenti nel database di CA SDM.

Indagine gestita

L'indagine gestita consente all'amministratore di CA SDM di selezionare un campione di popolazione per l'indagine e associarlo a un'indagine specifica. L'amministratore può quindi distribuire le richieste di specifiche indagini agli interessati per accettare la richiesta in un dato momento. Questa funzione consente all'amministratore di creare periodi di indagine aperti, pur mantenendo la possibilità di disporre di indagini basate sulle attività e sulle categorie correlate alle richieste, agli ordini di cambiamento e alle questioni.

Lo scopo delle indagini gestite è fornire un meccanismo per la gestione delle indagini. Questa funzione può essere utile per i moduli di indagine che devono essere monitorati di tanto in tanto, ad esempio le indagini utilizzate solo durante un breve periodo dell'anno o le indagini che sono rimaste troppo a lungo inattive.

Importante. Se si desidera inviare l'indagine a un numero elevato di contatti, impostare un valore predefinito di NX_SURVEY_ILIMIT in NX.env più alto, ad esempio 1073741824.

Nota: per ulteriori informazioni sulla creazione di indagini gestite, consultare la *Guida in linea*.

Servizi Web

I servizi Web sono conformi a standard per lo scambio di dati, che :

- Permettono le comunicazioni tra le applicazioni utilizzando il protocollo HTTP su vari server, a prescindere dall'ambiente operativo.
- Consentono alla maggior parte delle applicazioni di accedere alle funzioni del prodotto CA.
- Consentono ai client dei servizi Web di creare ticket, aggiornare gli asset, eseguire ricerche nell'archivio della conoscenza e altro ancora.

Nota: per ulteriori informazioni, consultare la sezione relativa alla gestione dei servizi Web nella *Guida all'implementazione*.

Capitolo 8: Configurazione degli account utente

Questa sezione contiene i seguenti argomenti:

Contatti (a pagina 319)
Definizioni dei contatti (a pagina 319)
Gruppi (a pagina 321)
Tipi contatto (a pagina 322)
Tipi di gestione speciali (a pagina 323)

Contatti

Una fase importante della definizione di un servizio è la definizione degli utenti che dovranno accedere a tale servizio. In CA SDM gli utenti sono denominati *contatti* ed è possibile eseguire diverse attività per impostarli e gestirli:

- Configurazione manuale dei contatti.
- Organizzazione dei contatti in gruppi che definiscono le aree di responsabilità.
- Definizione dei tipi di contatto per organizzare i contatti di CA SDM in gruppi logici in base all'uso che fanno del sistema.
- Importazione delle informazioni utente LDAP in un record contatto CA SDM.
- Assegnazione di un contatto ad un ruolo per definire la funzionalità del sistema accessibile.
- Assegnazione ad un contatto di un tipo di gestione speciale, quale VIP (Very Important Person).

Definizioni dei contatti

Tutti gli utenti che utilizzano CA SDM devono essere definiti come contatto. Il record di contatto di un utente definisce le informazioni utente richieste dal sistema, come indicato di seguito:

Identificazione di base

Definisce l'identificazione di base, ad esempio il nome e il tipo di contatto dell'utente. Il nome di un contatto viene utilizzato come identificativo principale quando si seleziona un contatto o quando si inseriscono le informazioni sul contatto in altri contesti.

Accesso

Definisce le informazioni di accesso, quali l'ID utente e, in alcuni casi, un campo PIN da utilizzare come password per la verifica dell'utente all'accesso. L'ID utente viene utilizzato per identificare l'utente nella tabella dei contatti a scopo di autenticazione e per determinare i tipi di accesso assegnati all'utente. In base alla configurazione di protezione eseguita dall'amministratore, è possibile specificare come campo PIN un altro campo, ad esempio ID contatto, che l'utente può utilizzare come password per l'accesso.

Protezione

Definisce il tipo di accesso assegnato nel record contatto o da un tipo di accesso predefinito, in base alla configurazione della protezione per il sistema. Il tipo di accesso di un utente può inoltre essere assegnato in base all'appartenenza ad un gruppo di directory LDAP.

Il tipo di accesso dell'utente determina tutti gli aspetti della protezione, incluso il metodo di autenticazione dell'utente, quale interfaccia può utilizzare e a quali funzioni del prodotto può accedere.

La gestione della protezione è una funzione dell'interfaccia Web.

Tipo di servizio

Determina il livello di servizio ricevuto da un utente. Il tipo di servizio del contatto definisce il livello di servizio che dovrebbe essere assegnato all'utente. Gli SLA (Service Level Agreement) vengono negoziati con i clienti di CA SDM e i tipi di servizio vengono utilizzati da CA SDM come meccanismo per l'implementazione degli SLA. Associando un tipo di servizio al record contatto di un utente, si garantisce che, quando viene creato un ticket per cui l'utente viene identificato come l'utente finale interessato, la qualità del tipo di servizio per il ticket sia almeno quella definita per il tipo di servizio del contatto.

L'impostazione degli SLA utilizzando i tipi di servizio è una funzione che, come amministratore, verrà eseguita utilizzando l'interfaccia Web.

Assegnazione automatica

Definisce le informazioni sull'assegnazione automatica, ad esempio i turni e la disponibilità (solo per i tipi di contatto analista). È possibile configurare i contatti di tipo analista per determinare se sono idonei all'assegnazione automatica. L'assegnazione automatica è valida solo per le richieste e viene definita come parte della definizione dell'area richiesta. È collegata anche ai gruppi a cui appartiene l'analista.

Modalità di invio dei messaggi di notifica agli utenti

Definisce le informazioni di notifica di un contatto, tra cui:

- diversi indirizzi di posta elettronica e numeri di telefono da utilizzare per la notifica
- metodo da utilizzare per le notifiche con livelli di urgenza diversi
- turni di lavoro durante i quali verranno ricevute le notifiche

Per il calcolo di ritardo della notifica viene considerato il fuso orario di contatto. Se il fuso orario del contatto non viene impostato, verrà utilizzato il fuso orario del server. L'utilizzo del fuso orario del server può comportare l'attivazione di notifiche al di fuori delle impostazioni del turno di lavoro.

Le informazioni sull'organizzazione, ad esempio la posizione, il tipo di organizzazione e il dipartimento, consentono di raggruppare i contatti in base all'organizzazione di appartenenza. Ad esempio, l'associazione di un contatto a una posizione, collega il contatto a un indirizzo fisico e facilita l'operazione di assegnazione automatica. È possibile assegnare l'organizzazione a un tipo di servizio, facilitando in tal modo la gestione degli SLA in base all'organizzazione piuttosto che per singoli contatti.

Gruppi a cui appartiene l'utente

È possibile organizzare i contatti in gruppi che rappresentano specifiche aree di responsabilità nel service desk. È possibile configurare e definire i contatti utilizzando l'interfaccia Web.

Gruppi

Un gruppo è una raccolta di contatti che condividono un'area comune di responsabilità. In CA SDM, i gruppi vengono implementati utilizzando il tipo predefinito di contatto gruppo, pertanto un gruppo rappresenta semplicemente un particolare tipo di contatto. Le informazioni di base del gruppo sono uguali a quelle del contatto, ma i gruppi rappresentano uno degli elementi chiave per l'assegnazione automatica delle richieste. È possibile associare le aree richiesta, le ubicazioni e un turno a un gruppo. Questi attributi vengono utilizzati per determinare se e quando i contatti presenti nel gruppo possono accettare l'assegnazione automatica di una richiesta.

Nota: per informazioni sulla definizione dei gruppi, vedere la *Guida in linea*.

Tipi contatto

I tipi di contatto vengono utilizzati per organizzare gli utenti di CA SDM in gruppi logici, in base all'uso che fanno del sistema. Ad esempio, alcuni tipi di contatto predefiniti del sistema sono analista, cliente e gruppo. Questi tipi di contatto predefiniti soddisfano le esigenze della maggior parte delle implementazioni di CA SDM. In determinate circostanze è invece possibile modificare i tipi di contatto predefiniti e crearne di nuovi. Quando gli utenti vengono definiti come contatti, è possibile associare un tipo di contatto ad ognuno di essi.

Nota: per ulteriori informazioni sulla definizione dei tipi di contatto, vedere la *Guida in linea*.

Comportamento in base al tipo di contatto

Il *tipo* di contatto determina quali contatti visualizzare (e le autorizzazioni correlate) nelle varie situazioni. Ad esempio, quando si esegue l'assegnazione manuale di qualsiasi tipo di ticket, ad esempio una richiesta oppure una questione, il campo nel quale specificare l'assegnatario presuppone che la persona specificata abbia il tipo di contatto analista. Se per tale campo si decide di selezionare un contatto da un elenco, nell'elenco di selezione vengono riportati solo i contatti di tipo analista. Se si specifica un contatto di tipo differente, viene visualizzata solo la schermata per la ricerca dell'analista.

Nota: una caratteristica importante relativa al tipo di contatto consiste nella possibilità di implementare i gruppi di contatti tramite il tipo di contatto del gruppo predefinito.

Configurazione della notifica in base al tipo di contatto

È possibile basare la notifica sul tipo di contatto, cosa che consente di inviare un messaggio di notifica a tutti i contatti di un determinato tipo.

Ulteriori informazioni:

Notifiche (a pagina 189)

Selezione dei contatti in base al tipo di contatto

È possibile selezionare gli utenti in base al tipo di contatto in vari contesti. Ad esempio, la maggior parte delle finestre di elenco e di selezione che visualizzano i contatti contiene un campo di ricerca in cui è possibile selezionare un tipo di contatto come criterio di ricerca.

Tipi di gestione speciali

È possibile definire tipi di gestione speciale che identificano contatti che richiedono una particolare attenzione. È possibile utilizzare i tipi di gestione speciale forniti da CA SDM oppure crearne di propri. È possibile visualizzare e individuare ticket che specificano un utente finale interessato che richiede particolare attenzione. Ad esempio, gli analisti possono visualizzare la cartella VIP nel contatore per individuare i ticket con utente finale VIP.

Di seguito si riportano alcuni esempi dei contatti che possono essere identificati dai tipi di gestione speciale:

- VIP (persone importanti), ad esempio i dirigenti
- Clienti con rinnovo di supporto in corso
- Clienti disabili che richiedono una gestione o attrezzature speciali
- Visitatori
- Contatti sospettati di utilizzo improprio o abuso di risorse di sistema

Quando a un contatto vengono assegnati uno o più tipi di gestione speciale, i ticket che specificano il contatto nel campo Utente finale interessato mostrano un banner di avviso, un'icona di avviso o entrambi. È possibile utilizzare i campi dei ticket e i tipi di gestione speciale per tenere traccia dei ticket, distinguendo tra due tipi di contatto correlati ma possibilmente distinti. Ad esempio, un VIP (Utente finale interessato) ha un assistente (Richiedente) che agisce per suo conto. Quando l'utente finale interessato è rappresentato da un contatto assegnato a un tipo di gestione speciale di VIP, l'analista può rendere prioritari i ticket in modo più accurato.

Ulteriori informazioni:

Modalità di configurazione di contatti di gestione speciale (a pagina 324)
Associazione di un contatto con un tipo di gestione speciale (a pagina 325)
Dati di directory LDAP (a pagina 326)

Modalità di configurazione di contatti di gestione speciale

Per configurare contatti di gestione speciale, procedere come segue:

1. Creare tipi di gestione speciale.
2. Associare un contatto a uno o più tipi di gestione speciale (a pagina 325). Analogamente, un tipo di gestione speciale può essere associato a più contatti.

   Un contatto associato a uno o più tipi di gestione speciale è distinto visivamente nel modulo Dettagli contatto e nel browser Profilo rapido da un banner visualizzato nella parte superiore di ogni pagina. Nel banner è visualizzata l'icona di avviso e il testo di avviso per ogni tipo di gestione speciale assegnato al contatto.

   Inoltre, i ticket che identificano il contatto come Utente finale interessato sono contrassegnati nei seguenti modi:

   - Visualizzazione di icone di avviso e di testo di avviso in un banner nella parte superiore del modulo dei dettagli del ticket.
   - Visualizzazione di icone di avviso nell'elenco dei ticket.
   - Inclusione nel contatore di cartelle e cartelle secondarie VIP per ciascun tipo di ticket. La cartella secondaria VIP include i ticket per gli utenti finali interessati classificati come contatti VIP con gestione speciale.

     Nota: la cartella di contatore VIP viene visualizzata per gli utenti con ruolo di analista.

Ulteriori informazioni

Associazione di un contatto con un tipo di gestione speciale (a pagina 325)
Dati di directory LDAP (a pagina 326)

Associazione di un contatto con un tipo di gestione speciale

È possibile assegnare un tipo di gestione speciale a un contatto per segnalare agli analisti ticket che riguardano utenti finali con particolari esigenze, ad esempio un utente con problemi di vista, un contatto che costituisce un rischio per la protezione e così via.

Per associare un contatto con un tipo di gestione speciale

1. Selezionare la scheda Dettagli contatto nella pagina Gestione speciale.

   Nella scheda Elenco gestione speciale associata sono elencati i tipi di gestione speciale associati al contatto.

2. Fare clic sul pulsante Aggiorna gestioni speciali del contatto.

   Viene visualizzato il filtro di ricerca.

3. Cercare il tipo di gestione speciale da associare al contatto.

   Viene visualizzata la pagina di aggiornamento delle gestioni speciali.

4. Selezionare uno o più tipi di gestione dalla colonna di sinistra e utilizzare il pulsante di spostamento (>>) per spostare i tipi nella colonna di destra. Fare clic su OK.

   Nota: è possibile rimuovere un'associazione da un contatto utilizzando il pulsante di spostamento (<<) per spostare il tipo di gestione speciale dalla colonna di destra in quella di sinistra. È possibile fare clic sull'icona di ricerca per cercare il valore desiderato.

   Il contatto viene associato al tipo di gestione.

   Quando un ticket specifica il contatto nel campo Utente finale interessato, in CA SDM viene visualizzato uno dei seguenti elementi, a seconda del tipo di gestione speciale associato :

   - Nei dettagli del contatto viene visualizzato un banner di avviso per l'utente finale interessato di un ticket.
   - Un testo di avviso viene visualizzato come banner nella parte superiore della pagina dei dettagli del ticket e in Profilo rapido.
   - Negli elenchi dei ticket la riga del contatto è evidenziata e contrassegnata con un flag di avviso.
   - La cartella V.I.P. viene visualizzata nel contatore per gli utenti con ruolo di analista. Tale cartella contiene tutti i ticket che sono associati a contatti (Utenti finali interessati) con un tipo di gestione speciale VIP.

Dati di directory LDAP

LDAP (Lightweight Directory Access Protocol) è un protocollo per le comunicazioni di rete che consente di eseguire query e di apportare modifiche ai servizi directory in esecuzione su una rete TCP/IP. Una directory LDAP è una struttura ad albero che contiene voci per la gestione di utenti, gruppi, computer, stampanti ed altre entità in una rete.

CA SDM può essere configurato per accedere ad una directory LDAP, che consente di utilizzare i dati LDAP in diversi modi:

- Sincronizzare i contatti con i record utente LDAP. La sincronizzazione può verificarsi nei seguenti modi:
  - **Al momento dell'accesso**: quando un utente accede al prodotto, se esiste un record LDAP per tale utente ma non un record contatto corrispondente, ne viene automaticamente creato uno in base alle informazioni LDAP.
  - **Nuovo contatto***:* quando si crea manualmente un record contatto, è possibile selezionare un record LDAP e unirne i valori di attributo ai relativi campi corrispondenti nel nuovo record contatto.
  - **Aggiornamento in batch**: è possibile eseguire processi batch per rendere automatiche le operazioni di importazione e aggiornamento dei record contatto con le informazioni provenienti dai record LDAP corrispondenti.

    Nota: la sincronizzazione con LDAP è un processo unidirezionale. I dati LDAP possono essere utilizzati per creare ed aggiornare i contatti, ma il prodotto non supporta aggiornamenti alla directory LDAP.

- Assegnare i tipi di accesso CA SDM in base all'appartenenza al gruppo LDAP.
- Implementare un metodo alternativo di esecuzione dell'autenticazione CA SDM.

Il componente ldap_virtb fornisce funzionalità di integrazione LDAP sui server seguenti a seconda della configurazione di CA SDM in uso, indipendentemente dal tipo di sistema operativo:

- Convenzionale: server primario o secondario.
- Disponibilità avanzata: server in background o server applicazioni.

Nota: Per ulteriori informazioni su componente ldap_virtb, consultare la *Guida all'implementazione*. Nel file $NX_ROOT/bopcfg/majic/ldap.maj è specificata l'associazione tra gli attributi LDAP e gli attributi dei record contatto.

Importante. In CA SDM è necessario che i record LDAP contengano una voce nel campo del cognome che consente di cercare, visualizzare e importare i dati LDAP.

Importante. CA SDM supporta la *ricerca per pagina*, che consente di ricercare tutti i record nella directory LDAP. La ricerca per pagina consente inoltre di importare i nuovi record contatto o i record contatto sincronizzati esistenti da qualsiasi numero di record LDAP. Queste funzionalità sono limitate, tuttavia, se si utilizza Sun Java System Directory Server o Novell eDirectory in quanto i server LDAP non supportano le ricerche per pagina. In tal caso, è solo possibile cercare, importare ed eseguire la sincronizzazione con il numero di record LDAP specificato da NX_LDAP_MAX_FETCH. Per ulteriori informazioni sulle ricerche per pagina, consultare il file NX.env (a pagina 341).

Configurazione delle opzioni LDAP

È possibile configurare CA SDM in modo che acceda ai dati di una directory LDAP.

Per configurare CA SDM in modo che acceda ai dati di una directory LDAP

1. Installare manualmente le opzioni LDAP utilizzando Gestione opzioni dell'interfaccia Web.

   Nota: le opzioni necessarie per l'integrazione di base di LDAP vengono identificate come obbligatorie nella colonna Descrizione della seguente tabella. Le opzioni identificate come facoltative sono funzioni che è possibile aggiungere solo se sono state installate tutte le opzioni richieste. I valori specificati quando si installano queste opzioni sono scritti nel file $NX_ROOT/NX.env. Per ulteriori informazioni sulle opzioni LDAP e sulle istruzioni per installarle, vedere la *Guida in linea.*

2. Riavviare il servizio CA SDM.

   Le modifiche vengono applicate.

Opzione	Valore predefinito	Descrizione
default_ldap_tenant		Richiesta per l'installazione multi-tenancy. Specifica l'assegnazione titolare predefinita per i contatti importati da LDAP. È necessario utilizzare l'UUID titolare quando si imposta il campo Valore opzione. **Nota:** è possibile ottenere l'UUID titolare da una query del database. Ad esempio, SELECT * FROM ca_tenant.
ldap_enable	Sì	Richiesto. Consente l'integrazione di LDAP con CA SDM.
ldap_host		Richiesto. Specifica il nome host o l'indirizzo IP del server di database LDAP.
ldap_port	389	Richiesto. Consente di specificare il numero di porta del server LDAP.
ldap_dn		Richiesto. Specifica il nome distinto di accesso del server LDAP. **Esempio**: CN=Joe, CN=Users, DC=KLAND, DC=AD, DC=com Se il server LDAP supporta i binding anonimi, è possibile non specificare questo valore.
ldap_pwd		Richiesto. Specifica la password per il nome distinto di accesso del server LDAP. Se il server LDAP supporta i binding anonimi, è possibile non specificare questo valore.
ldap_search_base		Richiesto. Consente di specificare il punto di partenza per le ricerche nella struttura dello schema LDAP: (UNIX) È necessario specificare un contenitore iniziale. Ad esempio: CN=Users, DC=KLAND, DC=AD, DC=com (Windows) Non è necessario specificare un contenitore. È possibile iniziare dalla parte superiore della struttura dello schema. Ad esempio: DC=KLAND, DC=AD, DC=com
ldap_filter_prefix	(&(objectClass= user)	Specifica il prefisso applicato ad un filtro generato automaticamente durante la ricerca degli utenti LDAP. **Nota:** questa variabile è stata sostituita dall'opzione ldap_user_object_class. Non è disponibile in Gestore opzioni, ma può essere impostata manualmente nel file NX.env.

Opzione	Valore predefinito	Descrizione
ldap_filter_suffix	)	Specifica il suffisso applicato ad un filtro generato automaticamente durante la ricerca degli utenti LDAP. **Nota:** questa variabile è stata sostituita dall'opzione ldap_user_object_class. Non è disponibile in Gestore opzioni, ma può essere impostata manualmente nel file NX.env.
ldap_user_object_ classe	persona	Richiesto. Specifica il valore dell'attributo LDAP objectClass applicato ad un filtro generato automaticamente durante la ricerca di utenti LDAP.
ldap_enable_group	Sì	Facoltativo. Consente l'assegnazione del tipo di accesso CA SDM in base all'appartenenza al gruppo LDAP.
ldap_group_object_ classe	gruppo	Richiesta solo se è installata l'opzione ldap_enable_group. Specifica il nome oggetto applicato ad un filtro generato automaticamente durante la ricerca dei gruppi.
ldap_group_filter_ prefisso	(&(objectClass= group)	Specifica il prefisso applicato a un filtro generato automaticamente durante la ricerca di gruppi LDAP. **Nota:** questa variabile è stata sostituita dall'opzione ldap_group_object_class. Non è disponibile in Gestore opzioni, ma può essere impostata manualmente nel file NX.env.
ldap_group_filter_ suffisso	)	Specifica il suffisso applicato a un filtro generato automaticamente durante la ricerca di gruppi LDAP. **Nota:** questa variabile è stata sostituita dall'opzione ldap_group_object_class. Non è disponibile in Gestore opzioni, ma può essere impostata manualmente nel file NX.env.
ldap_enable_auto	Sì	Facoltativo. Consente di generare automaticamente record contatto dai dati LDAP.
ldap_sync_on_null	Sì	Facoltativo. Sovrascrive gli attributi contatto di CA SDM con dati null se l'attributo utente LDAP corrispondente contiene un valore null.
ldap_service_type	Active Directory	Facoltativo. Utilizzare questa opzione se l'ambiente operativo di CA SDM è Windows e la directory LDAP *non* è Active Directory (ad esempio, eTrust o Novell). **Nota**: in un ambiente operativo UNIX, la funzionalità "Non AD" viene utilizzata solo se questa opzione *non* è installata. Se è installata, il tipo di servizio è impostato su Active Directory.

Opzione	Valore predefinito	Descrizione
ldap_enable_tls	No	Facoltativo. Consente di specificare se il protocollo TLS (Transport Layer Security) è attivato durante l'elaborazione LDAP.

Verifica dell'integrazione con LDAP

Dopo aver installato le opzioni LDAP necessarie, gli utenti CA SDM possono importare i dati LDAP caso per caso, eliminando in questo modo la necessità di inserire manualmente tutti i campi degli attributi del contatto.

Per verificare la corretta configurazione dell'integrazione con LDAP, completare i seguenti passaggi utilizzando l'interfaccia Web. Se si verificano problemi, consultare la sezione Risoluzione dei problemi (a pagina 340).

Per verificare che sia possibile cercare ed importare i record LDAP

1. Selezionare File, Nuovo contatto da LDAP nella scheda Service Desk.

   Viene visualizzata la finestra Ricerca Directory LDAP.

2. Specificare i criteri del filtro e fare clic su Cerca. Ad esempio, è possibile immettere b% nel campo Cognome per recuperare un elenco di utenti LDAP i cui cognomi iniziano con la lettera B.

   Nota: se la directory LDAP contiene migliaia di voci e non si limita la ricerca, la richiesta potrebbe tentare il recupero di *tutti* i record utente della directory LDAP. Ciò può causare il timeout della richiesta e la restituzione di zero record.

   Vengono visualizzati i risultati di ricerca corrispondenti ai criteri di filtro.

3. Selezionare una voce.

   Viene visualizzata la finestra Crea nuovo contatto, che contiene i valori degli attributi LDAP importati.

4. Fare clic su Salva.

   Viene creato il record contatto.

Per verificare che sia possibile aggiornare un contatto utilizzando i dati LDAP

Nota: prima di eseguire questa procedura, per scopi di test potrebbe essere necessario utilizzare uno strumento di modifica LDAP disponibile per modificare uno o più valori di attributi nella voce utilizzata per la procedura precedente. È possibile verificare se il contatto è aggiornato con i dati LDAP più recenti.

1. Selezionare Ricerca, Contatti nella scheda Service Desk.

   Viene visualizzata la finestra Ricerca contatto.

2. Specificare i criteri di filtro per la ricerca di un contatto con una voce utente LDAP corrispondente. È ad esempio possibile cercare il contatto creato nella procedura precedente.

   Vengono visualizzati i risultati di ricerca corrispondenti ai criteri di filtro.

3. Selezionare il contatto da aggiornare con i dati LDAP.

   Viene visualizzata la pagina Dettagli contatto contenente le informazioni sul contatto CA SDM.

4. Fare clic su Modifica.

   Viene visualizzata la pagina Aggiorna contatto.

5. Fare clic su Unisci LDAP.

   Viene visualizzata la pagina Elenco Voci LDAP contenente un elenco di tutte le voci utente LDAP corrispondenti al contatto CA SDM selezionato.

   Per cercare altre voci nella directory LDAP, è possibile fare clic su Mostra filtro, specificare i criteri di filtro e fare clic su Cerca.

   Nota: se la directory LDAP contiene migliaia di voci e non si limita la ricerca, la richiesta potrebbe tentare il recupero di *tutti* i record utente della directory LDAP. Ciò può causare il timeout della richiesta e la restituzione di zero record.

6. Fare clic sulla voce LDAP desiderata.

   Viene visualizzata la pagina Dettagli LDAP contenente i valori di attributo relativi alla voce selezionata. Verificare di aver selezionato la voce corretta per il contatto da aggiornare, quindi fare clic su Chiudi finestra.

7. Nella pagina Elenco Voci LDAP fare clic con il pulsante destro del mouse sulla voce che meglio corrisponde al contatto da aggiornare e scegliere Unisci nel contatto.

   Viene nuovamente visualizzata la pagina Aggiorna del contatto contenente i valori di attributo LDAP correnti. Se i dati LDAP sono stati modificati dalla creazione o dall'ultimo aggiornamento del contatto, le modifiche vengono applicate anche ai campi degli attributi del contatto.

Nota: se è stata installata l'opzione ldap_sync_on_null e la voce LDAP contiene valori Null per i campi degli attributi che corrispondono agli attributi del contatto che attualmente contengono valori, i valori del record contatto vengono sovrascritti con i valori Null al momento del salvataggio dei dati del contatto.

8. Fare clic su Salva nella pagina Aggiorna del contatto.

   Il contatto viene aggiornato con i dati LDAP corrispondenti.

Creazione automatica di un contatto

È possibile configurare CA SDM per creare automaticamente un contatto da un record utente LDAP corrispondente ogni volta che un nuovo utente accede CA SDM.

Per attivare questa funzionalità, installare tutte le opzioni LDAP richieste più l'opzione ldap_enable_auto.

Il record di contatto viene creato automaticamente come segue:

1. Se un utente che accede a CA SDM non dispone ancora di un record contatto, ma il suo nome di accesso è già presente in un record LDAP, i dati LDAP vengono automaticamente importati e viene creato un record contatto.
2. Il record contatto creato automaticamente eredita le impostazioni di protezione predefinite relative al tipo di accesso.
3. Al contatto può quindi essere assegnato in modo esplicito un tipo di accesso o il tipo di accesso può essere assegnato sulla base dell'appartenenza dell'utente ad un gruppo LDAP.

Questo processo è completamente trasparente all'utente, è infatti simile a qualsiasi altra sessione di accesso.

Assegnazioni del tipo di accesso dai gruppi LDAP

È possibile configurare CA SDM per assegnare automaticamente i valori del tipo di accesso ai contatti, in base all'appartenenza ai gruppi LDAP. Con l'assegnazione automatica del tipo di accesso abilitata, se un record utente LDAP utilizzato per creare un contatto appartiene ad un gruppo LDAP associato ad uno dei tipi di accesso CA SDM, al contatto viene assegnato automaticamente quel tipo di accesso. In caso contrario, il contatto eredita il tipo di accesso predefinito.

Per abilitare l'assegnazione automatica del tipo di accesso, è necessario installare le opzioni ldap_enable_group e ldap_group_object_class.

Nota: per informazioni dettagliate sull'installazione delle opzioni necessarie e sull'associazione dei gruppi LDAP ai tipi di accesso, vedere la *Guida in linea*.

Importazione in batch dei contatti con l'utilizzo di dati LDAP

È possibile eseguire l'utilità della riga di comando pdm_ldap_import per creare i contatti CA SDM in modalità batch utilizzando i dati LDAP.

Nota: oltre a creare contatti, pdm_ldap_import aggiorna quelli esistenti se non sono sincronizzati con le relative voci LDAP corrispondenti. È possibile utilizzare il processo batch pdm_ldap_sync per aggiornare i contatti esistenti, ma non per crearne.

La sintassi di pdm_ldap_import è la seguente:

```
pdm_ldap_import -l "ldap_where_clause" [-c "contact_where_clause"] [-u "userid"]
```

-l "*ldap_where_clause*"

Specifica gli ID utente dei record LDAP da cercare. Le variabili di sostituzione sono indicate dal carattere "?". Per *userid = ?* il valore predefinito è ad esempio *userid = ?*. In questo caso, l'ID viene associato all'attributo contatto ldap_dn.

Nota: utilizzare le parole chiave nel modo in cui sono definite nel file *ldap.maj*. È possibile effettuare una ricerca anche mediante la sintassi memberOf = 'group_dn'.

-c "*contact_where_clause*"

(Facoltativo) Specifica come determinare se il record contatto esiste già. Se il record contatto non esiste, ne viene inserito uno nuovo. Se il record contatto esiste e non è sincronizzato con i dati LDAP correnti, viene aggiornato.

-u "*userid*"

(Facoltativo) Specifica il nome di accesso con cui viene eseguito il programma pdm_ldap_import.

Nota: per specificare più record è possibile utilizzare caratteri jolly con pdm_ldap_import.

Esempi: importazioni in batch con i dati LDAP

In questo esempio viene importato un singolo record LDAP per l'ID utente jsmith11:

```
pdm_ldap_import -l "userid = 'jsmith11'"
```

In questo esempio vengono importati tutti i record LDAP con l'ID utente che inizia con la lettera C:

```
pdm_ldap_import -l "userid = 'c%'"
```

In questo esempio vengono importati tutti i record utente LDAP della directory:

```
pdm_ldap_import -l "userid = '%'"
```

Ulteriori informazioni:

Aggiornamento in batch dei contatti con l'utilizzo di dati LDAP (a pagina 336)

Importazione in batch dei contatti n base alla data e all'ora

È possibile configurare l'utilità pdm_ldap_import per importare i record LDAP creati prima o dopo una data e un'ora specificate. Per abilitare questa funzionalità, creare un file ldap.mod con il seguente contenuto:

```
OBJECT ldap {
  ATTRIBUTES LDAP_Entry {
    whenCreated whenCreated STRING ;
  };
};
```

L'attributo *whenCreated* viene aggiunto all'oggetto LDAP.

Di seguito sono indicate le regole per il filtraggio dei record utilizzando l'attributo whenCreated.

- Utilizzare solo l'operatore >= o <=.
- Specificare *tutti* i caratteri per il valore della data/ora, inclusa la Z. Inserire uno 0 in qualsiasi posizione da non dichiarare in modo esplicito, ad esempio l'ora del giorno.
- Inserire la specifica data/ora all'inizio del filtro. Non utilizzare 0 all'inizio della stringa.
- Non includere il secolo all'inizio. Per specificare ad esempio l'anno 2008, utilizzare 08.

Nota: il valore della data/ora deve essere racchiuso tra virgolette.

Esempio: utilizzo dell'attributo whenCreated per l'importazione di voci LDAP

Nel seguente esempio viene utilizzato l'attributo whenCreated per importare le voci LDAP create dopo il 11/03/08.

```
Pdm_ldap_import -l "whenCreated >= '080312000000Z'"
```

Esempio: utilizzo dell'attributo whenCreated per la ricerca di record LDAP

Nel seguente esempio viene utilizzato l'attributo whenCreated con pdm_ldap_test per cercare i record LDAP creati dopo il 11/03/08.

```
pdm_ldap_test.exe -f "whenCreated>=080312000000Z" -a whenCreated
Starting ldap_test.exe...
LDAP Directory Type : active directory
Service Desk Platform       : windows
Search Base : DC=kirklandsd,DC=ca,DC=com
Search Filter       : (&(objectClass=person)(whenCreated>=080312000000Z))
Administrator Username      :
CN=Administrator,CN=Users,DC=kirklandsd,DC=ca,DC=com
Administrator Password      : **********
LDAP Host   : gecko.kirklandsd.ca.com
LDAP Port   : 389
LDAP API Version    : 3
DN: CN=aixmail,CN=Users,DC=kirklandsd,DC=ca,DC=com
        whenCreated(17)(0): 20080312035327,0Z
DN: CN=hpmail,CN=Users,DC=kirklandsd,DC=ca,DC=com
        whenCreated(17)(0): 20080312035425,0Z
DN: CN=sunmail,CN=Users,DC=kirklandsd,DC=ca,DC=com
        whenCreated(17)(0): 20080312035726,0Z
3 Total LDAP records found...
```

Riepilogo dell'importazione in batch e dati del registro

Il comando pdm_ldap_import gestisce un registro dettagliato di tutte le attività di ogni esecuzione. Il file di registro ldap_logging.0-n si trova nella directory $NX_ROOT/log.

Di seguito è riportato un esempio dei dati di riepilogo restituiti da pdm_ldap_import alla riga di comando:

```
pdm_ldap_import Starting…
pdm_ldap_import Summary:  Processed(21) Updated(1) No Matches(7) New Contacts(11)
Multiple Matches(0) Empty Filter(2) Errors(0)
pdm_ldap_import Complete…
```

Nella seguente tabella sono descritti i dati di riepilogo.

Stato	Numero	Descrizione
Elaborati	21	Numero di contatti di CA SDM con voci LDAP corrispondenti.
Aggiornato	1	Numero dei record di contatto aggiornati in quanto le voci LDAP corrispondenti contenevano informazioni diverse.
Nessuna corrispondenza	7	Numero di record di contatto di CA SDM senza voci LDAP corrispondenti.

Stato	Numero	Descrizione
Nuovo contatto	11	Numero di nuovi record contatto creati in base alle voci LDAP corrispondenti
Più corrispondenze	0	Numero di voci LDAP con più record contatto corrispondenti, come definito dall'opzione ldap_search_base
Filtro vuoto	2	Numero di voci LDAP che non è possibile utilizzare per generare un filtro di ricerca valido
Errori	0	Numero di voci LDAP per le quali si è verificato un errore durante l'elaborazione. I record LDAP che non presentano un valore in un campo richiesto da CA SDM (ad esempio Cognome) vengono considerati errori e non possono essere importati.

Aggiornamento in batch dei contatti con l'utilizzo di dati LDAP

È possibile eseguire il comando pdm_ldap_sync per aggiornare i record contatto in modalità batch utilizzando i dati LDAP.

Importante Questa utilità sovrascrive il titolare esistente del contatto LDAP definito in CA SDM. Se si desidera mantenere il valore del titolare, è necessario modificare NX.env aggiungendo manualmente la variabile NX_RETAIN_TENANT_VALUE, impostandola su "Sì". Se questa variabile è impostata su "no", oppure non è presente o impostata in modo errato, l'utilità sovrascriverà le informazioni del titolare.

Nota: l'utilità pdm_ldap_sync sincronizza i contatti esistenti con le voci LDAP corrispondenti, ma non crea contatti. È possibile utilizzare il processo batch pdm_ldap_import per creare contatti.

La sintassi di pdm_ldap_sync è la seguente:

```
pdm_ldap_sync -l "ldap_where_clause" [-c "contact_where_clause"] [-u "userid"]
```

-l "ldap_where_clause"

Determina come cercare i record LDAP corrispondenti. Le variabili di sostituzione sono indicate dal carattere "?". Ad esempio, per *userid = ?*, il valore predefinito è *id = ?*. In questo caso, l'ID viene associato all'attributo Contact ldap_dn.

-c "contact_where_clause"

(Facoltativo) Determina i contatti utilizzati per la ricerca dei record LDAP corrispondenti.

Impostazione predefinita: "ldap_dn IS NOT NULL"

-u "userid"

(Facoltativo) Specifica l'ID utente con cui viene eseguito pdm_ldap_sync.

Nota: per specificare più record è possibile utilizzare caratteri jolly con pdm_ldap_sync.

Esempi:

L'esempio seguente definisce una baseline per i record di contatto che presentano un record LDAP corrispondente:

```
pdm_ldap_sync -l "userid = ?" -c ""
```

In questo esempio vengono utilizzati i parametri predefiniti per aggiornare tutti i contatti che presentano un nome distinto LDAP:

```
pdm_ldap_sync
```

In questo esempio viene aggiornato un singolo contatto:

```
pdm_ldap_sync -l "userid = ?" -c "userid = 'jsmith11'"
```

Ulteriori informazioni:

Importazione in batch dei contatti con l'utilizzo di dati LDAP (a pagina 333)

Riepilogo dell'aggiornamento in batch e dati del registro

Il comando pdm_ldap_sync gestisce un registro dettagliato di tutte le attività di ogni esecuzione. Il file ldap_logging.0-n si trova nella directory $NX_ROOT/log.

Di seguito è riportato un esempio dei dati di riepilogo restituiti da pdm_ldap_sync alla riga di comando:

```
pdm_ldap_sync Starting…
pdm_ldap_sync Summary:  Processed(21) Updated(1) No Matches(7) No Changes(11)
Multiple Matches(0) Empty Filter(2) Errors(0)
pdm_ldap_sync Complete…
```

Nella seguente tabella sono descritti i dati di riepilogo.

Stato	Numero	Descrizione
Elaborati	21	Numero di contatti di CA SDM con voci LDAP corrispondenti
Aggiornato	1	Numero di voci LDAP che presentano informazioni diverse rispetto a quelle dei record contatto di CA SDM corrispondenti
Nessuna corrispondenza	7	Numero di record di contatto di CA SDM senza voci LDAP corrispondenti.
Nessuna modifica	11	Numero di voci LDAP che presentano informazioni uguali a quelle dei record contatto di CA SDM corrispondenti
Più corrispondenze	0	Numero di voci LDAP con più record contatto corrispondenti in CA SDM, come definito dall'opzione ldap_search_base

Stato	Numero	Descrizione
Filtro vuoto	2	Numero di voci LDAP che non è possibile utilizzare per generare un filtro di ricerca valido
Errori	0	Numero di voci LDAP per le quali si è verificato un errore durante l'elaborazione.

Autenticazione tramite LDAP

È possibile utilizzare LDAP per autenticare gli utenti che accedono a CA SDM. L'autenticazione LDAP è disponibile quando il componente di autenticazione <EEM> viene integrato con <USDK> e sostituisce il metodo di validazione predefinito eseguito dal sistema operativo host. L'autenticazione LDAP è valida solo quando <EEM> è configurato per l'uso di una directory LDAP esterna ed è stata selezionata l'autenticazione SO come tipo di validazione dell'utente in un record Tipo di accesso.

Quando una funzione CA EEM è attivata, le richieste di accesso vengono controllate con il server CA EEM. Una richiesta di accesso viene autorizzata solo se si verifica quanto segue.

- L'ID utente specificato corrisponde ad un record contatto CA SDM.
- L'ID utente corrisponde ad un profilo utente in CA EEM.
- CA EEM convalida la combinazione ID utente/password.

Nota: Per ulteriori informazioni sull'utilizzo di CA EEM per l'autenticazione e su come spostare il modulo di autenticazione su un server esterno, consultare la *Guida all'implementazione*. Per ulteriori informazioni sulla configurazione del tipo di accesso, consultare la *Guida in linea*.

Transport Layer Security

È possibile configurare CA SDM per l'uso di TLS (Transport Layer Security) durante l'elaborazione di LDAP. TLS, un protocollo per le comunicazioni protette, rappresenta il successore di SSL v3 (Secure Socket Layer) nell'ambito della protezione. Per abilitare tale protocollo è necessario installare l'opzione ldap_enable_tls.

Importante Se questa funzione è abilitata, tutte le comunicazioni tra CA SDM e il server LDAP server sono crittografate. Se questa funzione *non* è abilitata, tutte le comunicazioni di dati, inclusi l'account e la password amministrativi utilizzati per accedere al server LDAP, vengono inviati in testo non crittografato.

Nota: per informazioni sulla configurazione di TLS, fare riferimento alla documentazione relativa al sistema operativo e al server LDAP. Per informazioni sull'utilizzo dell'opzione ldap_enable_tls, vedere la *Guida in linea*.

Mapping degli attributi

I valori degli attributi dei record contatto CA SDM vengono sincronizzati con i valori degli attributi utente LDAP in base alle definizioni di mapping degli attributi presenti nel file $NX_ROOT/bopcfg/majic/ldap.maj.

Il mapping viene illustrato dal seguente estratto da ldap.maj. I nomi attributo nella colonna sinistra (id) sono i nomi attributo dei contatti CA SDM. La colonna centrale (distinguishedName) contiene i nomi degli attributi LDAP corrispondenti.

```
    id               distinguishedName              STRING 512;
last_name         sn,pzLastName                    STRING ;
first_name        givenName,pzFirstName            STRING ;
middle_name     initials,pzMiddleName           STRING ;
userid              uid,sAMAccountName,pzUserName     STRING ;
phone_number    telephoneNumber,pzWorkPhoneNumber STRING ;
```

Se esiste un attributo SREL (una singola relazione o chiave esterna in un'altra tabella del database) su CA SDM, il valore attributo del contatto viene sincronizzato con il valore LDAP corrispondente. Se l'attributo SREL non esiste, non viene creato automaticamente durante l'elaborazione della sincronizzazione LDAP.

Nota: per impostazione predefinita, il mapping degli attributi viene configurato per lo schema LDAP di Microsoft Active Directory. Se necessario, è possibile modificare il mapping utilizzando un file mod.

Modalità di modifica dell'associazione dell'attributo

È possibile modificare l'associazione dell'attributo predefinita.

Per modificare l'associazione dell'attributo predefinita, attenersi alla procedura seguente:

1. Accedere a $NX_ROOT/site/mods/majic e aprire il file mod.
2. Utilizzare le istruzioni MODIFY nel file mod, come descritto di seguito.
   - Le istruzioni MODIFY devono sempre trovarsi in prima posizione nel file.
   - Dopo le istruzioni MODIFY, tutti i campi aggiuntivi che non si trovano nel file ldap.maj devono essere inseriti utilizzando la sintassi mostrata nel seguente esempio.
   - Se si definisce un campo che contiene un trattino nel nome attributo, il nome deve essere inserito tra virgolette. In caso contrario, quando si crea il file mod l'attributo causerà un errore di sintassi. Il nome attributo seguente deve ad esempio essere inserito tra virgolette:

     ```
     c_nx_string1 'swsd-secret-question' STRING ;
     ```

3. Salvare e chiudere il file mod.
4. Riavviare il servizio CA SDM.

   Importante Se viene rilevata una differenza nella sintassi o nell'uso di maiuscole e minuscole, il motore Web non viene avviato.

   Le modifiche diventano effettive.

Esempio: utilizzo delle istruzioni MODIFY

L'esempio seguente mostra come modificare due campi e aggiungere un campo nuovo:

```
//
// Associazione dell'attributo userid di CA SDM all'ID utente ADAM
//
MODIFY ldap userid cn ;
MODIFY ldap middle_name middleName ;
OBJECT ldap LDAP {
ATTRIBUTES LDAP_Entry{
contact_num employeeNumber STRING ;
};
} ;
```

Risoluzione dei problemi

Per la risoluzione dei problemi relativi alle comunicazioni con un server LDAP, occorre innanzitutto tenere presente che raramente esistono due implementazioni LDAP identiche. Per verificare che l'integrazione LDAP funzioni correttamente, è possibile utilizzare le utilità di CA SDM.

Nota: CA SDM è preconfigurato solo per l'integrazione con Microsoft Active Directory, eTrust e iPlanet. L'integrazione con altri server LDAP spesso richiede modifiche e adattamenti a entrambe le parti.

Visualizzazione dello stato dei daemon o dei processi

Il processo ldap_virtdb gestisce le interazioni tra CA SDM e il database virtuale LDAP.

Per visualizzare lo stato di tutti i processi o i daemon (UNIX) CA SDM

1. Eseguire pdm_status alla riga di comando senza parametri:

   ```
   pdm_status
   ```

   Il comando pdm_status mostra lo stato di tutti i daemon (UNIX) o processi (Windows) CA SDM presenti sul sistema nel quale viene eseguito, ad esempio:

   ```
   DAEMON                          STATUS      HOST      PID   SLUMP CONNECT TIME
   ------------------------------------------------------------------------------
   --
   Agent antfarm                  Running     antfarm   455   Tue Feb 17 17:55:12
   Ddict_rd              (ddictrd) Completed   antfarm
   Data Dictionary    (ddictbuild) Completed   antfarm
   ...
   User Validation       (boplgin) Running     antfarm   456   Tue Feb 17 17:55:21
   ```

2. Esaminare lo stato del processo ldap_virtdb nell'output del comando.

Comando slstat

Eseguire il seguente comando senza parametri per verificare che bopLDAP sia connesso:

```
slstat
```

Esaminare l'output del comando per verificare lo stato di bopLDAP.

File NX.env

Esaminare il file $NX_ROOT/NX.env per verificare che le opzioni LDAP di base siano state installate correttamente.

A seconda delle opzioni LDAP installate, il file NX.env dovrebbe includere righe simili alle seguenti:

```
@NX_LDAP_DN=qauser
@NX_LDAP_ENABLE=Yes
@NX_LDAP_ENABLE_AUTO=Yes
@NX_LDAP_HOST=myserver
@NX_LDAP_PORT=389
@NX_LDAP_PWD=OBUNQXo7CmgbThZlCiMKIwJlA3UXdVNAOjUpHjstfDt2LBIDPgwtWA==
@NX_LDAP_SEARCH_BASE=dc=mycontroller, dc=xyz, dc=com
@NX_LDAP_SERVICE_TYPE=Active Directory
@NX_LDAP_SYNC_ON_NULL=Yes
@NX_LDAP_USER_OBJECT_CLASS=person
```

Importante. I server SunOne Directory Server e Novell eDirectory non supportano le ricerca per pagina, pertanto la ricerca, l'importazione e la sincronizzazione LDAP sono limitate al valore dei record NX_LDAP_MAX_FETCH per chiamata. Il valore predefinito è 100. Se si utilizza uno di questi server LDAP, potrebbe essere necessario aggiungere NX_LDAP_MAX_FETCH al file NX.env per specificare il numero massimo di record LDAP. È possibile impostare NX_LDAP_MAX_FETCH su qualsiasi valore inferiore al valore di LDAP_SIZELIMIT_EXCEEDED o LDAP_ADMINLIMIT_EXCEEDED nel server LDAP.

Ulteriori informazioni:

Configurazione delle opzioni LDAP (a pagina 327)

pdm_ldap_test

Utilizzare l'utilità della riga di comando pdm_ldap_test per verificare la connessione ad una directory LDAP, che le opzioni di ricerca siano configurate correttamente e la configurazione TLS.

Per impostazione predefinita, pdm_ldap_test utilizza le impostazioni dei parametri immesse nel file $NX_ROOT/NX.env al momento dell'installazione, della modifica o della disinstallazione delle opzioni LDAP. Per ignorare le impostazioni predefinite, è possibile specificare i parametri alla riga di comando di pdm_ldap_test.

Per verificare i parametri disponibili per il comando, immettere il seguente comando:

```
pdm_ldap_test -h
```

Importante: in UNIX, LIBPATH deve essere impostato prima di eseguire diverse utilità di CA SDM. Utilizzare *pdm_task* per impostare LIBPATH prima di eseguire un'utilità. Immettere ad esempio "pdm_task pdm_clean_attachments...".

Verifica della connessione al server LDAP

Per verificare la connessione al server LDAP, eseguire pdm_ldap_test senza parametri:

```
pdm_ldap_test
```

Connessione riuscita al server LDAP

Se la connessione ha esito positivo, l'output ricevuto sarà simile al seguente:

```
Starting pdm_ldap_test...
Tipo servizio LDAP=active directory
Piattaforma Service Desk=windows
Using search base=DC=mycontroller,DC=xyz,DC=com
Uso filtro=(&(objectCategory=person))
ldap_init(myserver.mycontroller.xyz.com,389): (Success)
ldap_bind_s(Administrator) (Success)
API LDAP Versione 3
```

Connessione non riuscita - Server non accessibile o nome/porta non valido

Se la connessione non riesce per l'inattività del server oppure perché è stato specificato un nome o una porta non valida per il server LDAP, l'output restituito sarà simile al seguente:

```
Starting pdm_ldap_test...
Tipo servizio LDAP=active directory
Piattaforma Service Desk=windows
Using search base=DC=mycontroller,DC=xyz,DC=com
Uso filtro=(&(objectCategory=person))
ldap_init(junk,389): (Success)
ldap_bind_s(Administrator) (Server Down)
```

Connessione non riuscita - LDAP_DN o LDAP_PWD non valido

Se la connessione non riesce poiché sono stati specificati valori non validi per LDAP_DN o LDAP_PWD, l'output restituito sarà il seguente:

```
Starting pdm_ldap_test...
Tipo servizio LDAP=active directory
Piattaforma Service Desk=windows
Using search base=DC=mycontroller,DC=xyz,DC=com
Uso filtro=(&(objectCategory=person))
ldap_init(myserver.mycontroller.xyz.com,389): (Success)
ldap_bind_s(junk) (No Such Object or Invalid Credentials)
```

Visualizzazione dei parametri di ricerca

Per verificare che i parametri di ricerca siano configurati correttamente, eseguire pdm_ldap_test senza parametri:

```
pdm_ldap_test
```

Esecuzione corretta della ricerca

Se la ricerca viene eseguita correttamente, verrà restituito un output simile al seguente:

```
DN: CN=John A. Smith,CN=Users,DC=COMPUTERTEST
        c(2)(0):
        displayName(14)(0): John A. Smith
        mail(14)(0): account02@mycompany.com
        givenName(4)(0): John
        initials(1)(0): a
        distinguishedName(38)(0): CN=John a.

Smith,CN=Users,DC=COMPUTERTEST
        objectGUID(3)(0): 314738
        pager(12)(0): ###-111-1111
        postalCode(5)(0): 11111
        SAMAccountName(7)(0): account02
        sn(6)(0): Smith
        telephoneNumber(12)(0): ###-342-6265
        userPrincipalName(16)(0): account02@COMPUTERTEST

DN: CN=Mike Johnson,CN=Users,DC=COMPUTERTEST
        displayName(10)(0): Mike Johnson
        givenName(4)(0): Mike
        distinguishedName(34)(0): CN=Mike

Johnson,CN=Users,DC=COMPUTERTEST
        objectGUID(12)(0): 312328
        SAMAccountName(7)(0): account03
        sn(5)(0): Johnson
        userPrincipalName(16)(0): account03@COMPUTERTEST
```

Ricerca non riuscita - SEARCH_BASE non valido

Se la ricerca non riesce poiché il valore di SEARCH_BASE non è valido, l'output restituito dovrebbe essere il seguente:

```
Starting pdm_ldap_test...
Tipo servizio LDAP=edirectory
Piattaforma Service Desk=windows
Uso base di ricerca=o=SmartLabsx
Uso filtro=(&(objectClass=InetOrgPerson)
ldap_init(155.35.173.110,15389): (Success)

ldap_bind_s() (Success)
API LDAP Versione 3
ldap_search_st() (No Such Object or Referral)
```

Ricerca non riuscita - SIZELIMIT_EXCEEDED, TIMEOUT

La ricerca potrebbe non riuscire con conseguente visualizzazione di un messaggio SIZELIMIT_EXCEEDED o TIMEOUT se si specifica un filtro che non limita sufficientemente la ricerca. La maggior parte dei server LDAP limita le dimensioni dei risultati restituiti da una richiesta di ricerca. Se il limite viene superato, viene restituito un messaggio SIZELIMIT_EXCEEDED. Se l'esecuzione della ricerca impiega più di 20 secondi, che rappresenta il timeout predefinito, il server LDAP interrompe la richiesta e viene visualizzato un messaggio di errore TIMEOUT simile al seguente:

```
Starting pdm_ldap_test...
Tipo servizio LDAP=edirectory
Piattaforma Service Desk=windows
Uso base di ricerca=o=SmartLabsx
Uso filtro=(&(objectClass=InetOrgPerson)
ldap_init(155.35.173.110,15389): (Success)
ldap_bind_s() (Success)
API LDAP Versione 3
ldap_search_st() (TIMEOUT or SIZELIMIT_EXCEEDED)
```

Ricerca non riuscita - 0 record restituiti

La ricerca potrebbe non riuscire poiché il filtro predefinito non è valido. Se l'opzione ldap_test restituisce zero (0) record, controllare sempre la riga Using filter, che rappresenta il filtro di base generato dalle opzioni LDAP_FILTER_PREFIX e LDAP_FILTER_SUFFIX o LDAP_OBJECT_CLASS:

```
Starting pdm_ldap_test...
Tipo servizio LDAP=edirectory
Piattaforma Service Desk=windows
Uso base di ricerca=o=SmartLabs
Uso filtro=(&(objectClass=InetOrgPerson)
ldap_init(155.35.173.110,15389): (Success)
ldap_bind_s() (Success)
API LDAP Versione 3
ldap_search_st() 0 record
```

Limitazione della ricerca

Utilizzare il parametro -f con il comando pdm_ldap_test per specificare un filtro da aggiungere al filtro di base per limitare i criteri di ricerca. Nel filtro è necessario utilizzare la sintassi LDAP appropriata e i nomi di attributo dello schema LDAP. Racchiudere il filtro tra virgolette e utilizzare le parentesi per indicare l'ordine di precedenza dell'operatore.

Utilizzare ad esempio il comando seguente per ricercare tutti i record in cui sn=Account_10001:

```
pdm_ldap_test –f “(sn=Account_10001)”
```

L'utilità pdm_ldap_test supporta i seguenti operatori di uguaglianza:

Operatore di uguaglianza	Descrizione
=	uguale a
<=	minore di o uguale a
>=	maggiore di o uguale a
~=	simile a

L'utilità pdm_ldap_test supporta i seguenti operatori booleani:

Operatore booleano	Descrizione
&	E
|	oppure
!	NOT

Gli operatori AND e OR influenzano ogni set di parentesi () nel filtro di ricerca. L'operatore NOT influenza solo il primo set di parentesi. Questi operatori si trovano sempre *prima* dei filtri di ricerca e non tra di essi. Possono essere applicati ad un numero qualsiasi di filtri, come mostrato nei seguenti esempi:

```
“(&(sn=Brown)(initials=A)) “
```

```
“(|(sn=Brown)(sn=Smith))”
```

```
“(!sn=Brown)”
```

Come determinare i nomi di attributo contenenti valori

Utilizzare il parametro -a “*” e il parametro -f con il comando pdm_ldap_test per determinare quali attributi vengono definiti per i record di gruppi o utenti LDAP. Questo test è utile per determinare la presenza di attributi LDAP che è possibile associare agli attributi contatto e per verificare che uno specifico attributo contenga un valore e sia disponibile durante la creazione o l'aggiornamento dei record contatto.

Nel seguente esempio viene mostrato l'output di iPlanet Directory:

```
pdm_ldap_test -a "*" -f sn=Account_1000001

2 record LDAP trovato...

DN: cn=Account_1000001,ou=200K_Plus,o=SmartLabs
    sn(15)(0): Account_1000001
    objectClass(13)(0): inetOrgPerson
    objectClass(20)(1): organizationalPerson
    objectClass(6)(2): Person
    objectClass(18)(3): ndsLoginProperties
    objectClass(3)(4): Top

DN: cn=Account_1000001,ou=2_Plus,o=SmartLabs
    mail(28)(0): ThisIsTheMailingAddressField
    uid(13)(0): Login_1000001
    givenName(17)(0): GivenNameOfPerson
    sn(15)(0): Account_1000001
    objectClass(13)(0): inetOrgPerson
    objectClass(20)(1): organizationalPerson
    objectClass(6)(2): Person
    objectClass(18)(3): ndsLoginProperties
    objectClass(3)(4): Top
```

Nel seguente esempio viene mostrato l'output di Active Directory:

```
Ldap_test –a “*” –f (&(sn=Brown)(initials=A))”

1 record LDAP trovato...

DN: CN=John A. Smith,CN=Users,DC=mycontroller,DC=xyz,DC=com
    objectClass(3)(0): top
    objectClass(6)(1): person
    objectClass(20)(2): organizationalPerson
    objectClass(4)(3): user
    cn(16)(0): John A. Smith
    sn(5)(0): Brown
    givenName(7)(0): John
    initials(1)(0): A
    distinguishedName(55)(0): CN=John A.
    Smith,CN=Users,DC=mycontroller,DC=xyz,DC=com
    displayName(16)(0): John A. Smith
    memberOf(52)(0): CN=Domain Admins,CN=Users,DC=mycontroller,DC=xyz,DC=com
    sAMAccountName(7)(0): smijo04
    userPrincipalName(25)(0): smijo04@mydomain.xyz.com
    objectCategory(63)(0):
    CN=Person,CN=Schema,CN=Configuration,DC=mycontroller,DC=xyz,DC=com
```

Attivazione del tracciamento LDAP

Utilizzare l'utilità pdm_logstat per attivare la registrazione delle tracce per il monitoraggio dell'utilizzo di LDAP in CA SDM.

Il comando pdm_logstat presenta la seguente sintassi:

```
pdm_logstat -f ldap_virtdb.c 1000
```

I seguenti messaggi stdlog consentono di identificare lo stato del processo di connessione.

Come determinare se il processo ldap_virtdb è stato avviato

La prima riga da ricercare quando si esaminano i messaggi stdlog LDAP è quella relativa all'avvio del processo ldap_virtdb. LDAP viene riconosciuto in CA SDM solo con l'avvio di questo processo .

Nota: anche se le opzioni di integrazione con LDAP non sono installate o configurate, questo processo viene eseguito comunque.

```
06/03 17:00:18.27 cpasd1   bopLDAP      1964 SIGNIFICANT  ldap_virtdb.c

680 STARTUP of LDAP_virtdb
```

Come determinare se tutte le opzioni necessarie sono installate

Se una delle opzioni LDAP necessarie non è stata definita, stdlog mostra le opzioni mancanti, come illustrato nel seguente esempio:

```
06/03 17:00:18.72 cpasd1  bopLDAP  1964 SEVERE_ERROR ldap_virtdb.c  1023 LDAP Server
port id missing
06/03 17:00:18.78 cpasd1  bopLDAP  1964 SEVERE_ERROR ldap_virtdb.c  1023 LDAP Server
distinguished name missing
06/03 17:00:18.78 cpasd1  bopLDAP  1964 SEVERE_ERROR ldap_virtdb.c  1023 LDAP Server
distinguished name password missing
```

Come determinare se la connessione LDAP è riuscita

È possibile verificare se la connessione LDAP è riuscita esaminando le voci presenti in stdlog. Queste voci dovrebbero indicare l'avvenuta connessione con il server LDAP, come mostrato nel seguente esempio:

```
06/05 12:35:10.41 cpasd1   bopLDAP  1912 SIGNIFICANT  ldap_virtdb.c  958 LDAP_SRVR
connecting to host(Francisco.us.danconia.net) port(389)
06/05 12:35:11.01 frisco   bopLDAP  1912 SIGNIFICANT  ldap_virtdb.c 1002 LDAP_SRVR
binding with username(simon)
```

Come determinare se la connessione LDAP non è disponibile

Se per un motivo qualsiasi non è possibile stabilire una connessione con il server LDAP, le funzioni *Voci LDAP*, *Unisci LDAP* o qualsiasi altra funzione LDAP, viene disattivata e non viene restituito alcun risultato. In tal caso, quando si tenta di eseguire le operazioni, stdlog mostra messaggi simili ai seguenti:

```
06/03 17:00:32.25 cpasd1   bopLDAP  1964 SIGNIFICANT  ldap_virtdb.c   219 LDAP server not available; 'register_producer' not processed

06/05 10:52:57.63 cpasd1   bopLDAP  1896 SIGNIFICANT  ldap_virtdb.c   219 LDAP server not available; 'select_full' not processed

06/05 10:52:57.66 cpasd1   web:local 1868 ERROR   sel_data_cache.  611 Error in ldap Select_Cache method got_initial_count: LDAP server not available; 'select_full' not processed

06/05 10:52:57.66 cpasd1   bopLDAP  1896 SIGNIFICANT  ldap_virtdb.c   219 LDAP server not available; 'select_cancel' not processed
```

Come determinare il filtro utilizzato

CA SDM carica i record dalla directory LDAP a seconda della base di ricerca e del filtro definiti in Gestore opzioni e in base ai criteri di ricerca immessi dall'utente. Ricercare il messaggio seguente per determinare il filtro effettivo generato nella richiesta di ricerca:

```
06/24 14:18:28,32 mcxxx04- bopLDAP   3844 TRACE   ldap_virtdb.c   853 Starting select full: base=DC=kirklandsd,DC=ca,DC=com; filter=(&(objectCategory=person)(|(sn=Jones)(pzLastName=Jones))); attributes=(uid,sAMAccountName,pzUserName,distinguishedName)
```

Come determinare gli attributi caricati

CA SDM carica i record dalla directory LDAP a seconda della base di ricerca e del filtro definiti in Gestore opzioni. Ricercare il messaggio seguente per verificare la correttezza di SEARCH_BASE e dell'associazione dell'attributo, come definito in ldap.maj e ldap_group.maj:

```
06/24 14:18:28,39 mcxxx04- bopLDAP      3844 TRACE     ldap_virtdb.c    766 Starting select short: base=CN=John D. Jones,CN=Users,DC=kirklandsd,DC=ca,DC=com; filter=(&(objectCategory=person)); attributes=(modifyTimestamp,sn,pzLastName,givenName,pzFirstName,initials,pzMiddleName,uid,sAMAccountName,pzUserName,telephoneNumber,pzWorkPhoneNumber,mobile,pzMobilePhoneNumber,department,pzDepartment,facsimileTelephoneNumber,pzFaxPhoneNumber,pager,mail,pzEmailAddress,streetAddress,pzAddress,l,pzCity,st,pzState,postalCode,pzPostalCode,c,pzCountry,o,memberOf)
```

Come determinare quali sono i dati LDAP disponibili e non disponibili

Supponendo che CA SDM sia stato in grado di creare l'associazione con l'attributo ID dell'oggetto LDAP, vengono recuperati gli attributi (come definiti in $NX_ROOT/bopcfg/majic/ldap.maj) per ogni voce. In caso contrario, viene registrato un messaggio che informa della mancata definizione di un attributo. Di seguito è riportato un messaggio di esempio:

```
06/24 14:18:28.41 mclda04- bopLDAP      3844 TRACE   ldap_virtdb.c   1396 Value not
available for 'modifyTimestamp'

06/24 14:18:28.41 mclda04- bopLDAP      3844 TRACE   ldap_virtdb.c   1396 Value not
available for 'telephoneNumber,pzWorkPhoneNumber'
```

Capitolo 9: Gestione dei ruoli

Nota: per informazioni su altri aspetti dell'interfaccia Web, consultare Configurazione dell'interfaccia Web.

Questa sezione contiene i seguenti argomenti:

Ruoli (a pagina 351)
Ruoli predefiniti (a pagina 351)
Protezione Role-Based (a pagina 353)
Navigazione basata su ruoli (a pagina 363)
Modalità di implementazione di un ruolo personalizzato (a pagina 372)
Modalità di implementazione di una struttura menu personalizzata (a pagina 374)
Creazione di un record ruolo (a pagina 375)
Creazione di un record scheda (a pagina 376)
Creazione di un record barra dei menu (a pagina 377)
Creazione di record di modulo Web (a pagina 378)
Copia di una struttura menu (a pagina 379)
Creazione e personalizzazione di una struttura menu (a pagina 380)
Creazione e pubblicazione di un set di file della Guida (a pagina 381)
Cambio dei ruoli (a pagina 383)

Ruoli

I *ruoli* sono i record principali che controllano la protezione di CA SDM e la navigazione dell'interfaccia utente. Ogni ruolo definisce una visualizzazione specifica del sistema, che mostra solo le funzionalità necessarie agli utenti per eseguire le attività assegnate normalmente alla mansione che svolgono nella propria organizzazione aziendale.

Il ruolo predefinito di un utente determina quale visualizzazione di sistema compare all'accesso. Gli utenti a cui sono assegnati più ruoli possono passare da un ruolo a un altro per usare diverse visualizzazioni di sistema senza dover uscire e riaccedere.

Ruoli predefiniti

È possibile utilizzare i ruoli nella loro configurazione predefinita, modificarli in modo da soddisfare le esigenze aziendali o crearne di nuovi.

La seguente tabella descrive i ruoli predefiniti installati in CA SDM. Questi ruoli sono progettati in modo che siano allineati con le procedure ottimali ITIL v3, il che riduce il numero di personalizzazioni specifiche per i siti e necessarie all'organizzazione IT per essere conformi agli standard ITIL.

CA SDM supporta solo ITIL, e la documentazione di CA SDM è basata su ITIL. Per ulteriori informazioni, consultare Configurazione ITIL (a pagina 61).

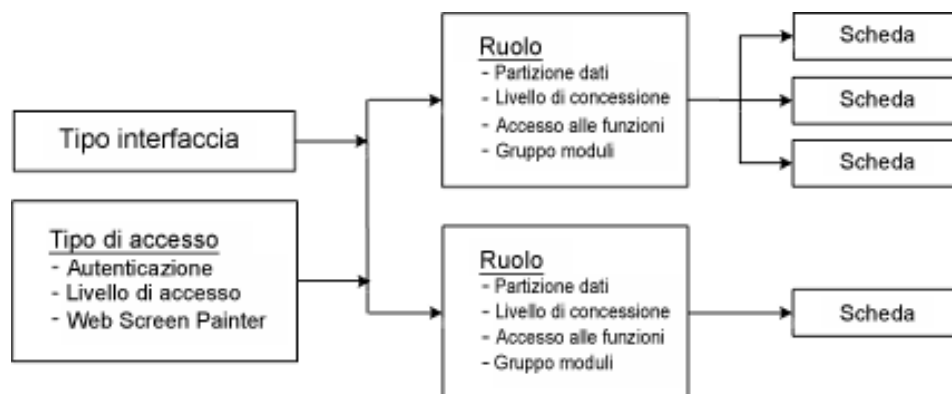
Tipo di ruolo	Nome ruolo	Descrizione
Utenti finali	Visualizzatore della configurazione	Esegue attività di ricerca e visualizzazione degli elementi della configurazione dall'interno dell'organizzazione.
	Cliente	Esegue attività self-service di base dall'esterno dell'organizzazione.
	Dipendente	Esegue attività self-service di base dall'interno dell'organizzazione.
Analisti	Analista della configurazione	Esegue attività all'interno del processo del ciclo di vita dell'elemento della configurazione e supporto CMDB di secondo livello all'interno dell'organizzazione.
	Rappresentante del servizio clienti	Fornisce assistenza a utenti esterni all'organizzazione, di solito clienti.
	Analista della conoscenza	Esegue attività all'interno del processo del ciclo di vita della gestione della conoscenza.
	Analista di livello 1	Fornisce assistenza di primo livello all'interno dell'organizzazione.
	Analista di livello 2	Fornisce assistenza di secondo livello all'interno dell'organizzazione, il che richiede conoscenze specifiche più approfondite.
	Analista automazione supporto	Fornisce assistenza di primo livello all'interno dell'ambiente di assistenza in tempo reale.
	Analista vendor	Fornisce supporto dall'esterno dell'organizzazione a un segmento limitato dell'ambiente IT, come ad esempio l'hardware specifico di un vendor.
Gestione	Gestione Cambiamento	Gestisce il processo degli ordini di cambiamento, senza però occuparsi, di solito, degli analisti che lavorano sui ticket di ordine di cambiamento.
	Gestione servizio clienti	Gestisce i rappresentanti del servizio clienti e il processo di assistenza esterno.
	Gestione Incidente	Gestisce il processo degli incidenti, senza però occuparsi, di solito, degli analisti che lavorano sui ticket di incidenti.
	Gestione della conoscenza	Supervisiona gli analisti della conoscenza, le riassegnazioni e le escalation relative ai documenti della conoscenza, nonché l'amministrazione della conoscenza giornaliera.

Tipo di ruolo	Nome ruolo	Descrizione
	Gestione problemi	Gestisce il processo dei problemi, senza però occuparsi, di solito, degli analisti che lavorano sui ticket di problemi.
	Gestione Service Desk	Gestisce le escalation e supervisiona gli analisti di livello 1. Può inoltre gestire le operazioni di service desk generiche.
Amministratori	Amministratore	Esegue attività amministrative in tutta l'implementazione CA SDM e Gestione della conoscenza. Normalmente questo ruolo installa, configura e integra i prodotti.
	Amministratore della configurazione	Esegue attività amministrative relative all'implementazione CA CMDB. Normalmente questo ruolo amministra l'infrastruttura degli elementi della configurazione e CMDB, nonché le strutture dei dati.
	Amministratore Gestione della conoscenza	Esegue la configurazione e il monitoraggio delle impostazioni di gestione delle conoscenza.
	Amministratore Service Desk	Esegue attività amministrative relative a dati e processi, come la creazione e l'aggiornamento delle categorie, dei contatti, dei tipi di servizio, delle cause principali e così via.
	Amministratore automazione supporto	Esegue attività amministrative relative all'ambiente Support Automation, come la configurazione delle code e delle autorizzazioni relative agli strumenti degli analisti.
	Amministratore del sistema	Esegue attività amministrative relative all'implementazione, all'adattamento e alla configurazione di CA SDM, come l'impostazione delle opzioni, la configurazione delle integrazioni e la modifica dei moduli Web.
	Amministratore titolari	Esegue attività amministrative relative alle funzionalità multi-tenancy.

Protezione Role-Based

I tipi di accesso e i ruoli sono i componenti primari utilizzati per il controllo della protezione di CA SDM.

Lo schema seguente mostra una panoramica delle relazioni tra ruoli e altri oggetti di sistema per garantire la protezione basata su ruoli.

Nota: per ulteriori informazioni sulla protezione, consultare Sicurezza (a pagina 282).

Modalità di funzionamento dei tipi di accesso

Ogni tipo di accesso per un utente controlla i seguenti aspetti del comportamento di sistema:

- Il modo in cui CA SDM esegue l'autenticazione Web quando l'utente accede al sistema
- Il livello di accesso per l'utente
- La possibilità da parte dell'utente di modificare i moduli Web o lo schema del database mediante Web Screen Painter
- Quali ruoli sono disponibili per l'utente

È possibile associare un tipo di accesso a un contatto selezionando il tipo di accesso quando si crea o aggiorna il record contatto.

La seguente tabella elenca i tipi di accesso predefiniti, ne identifica i ruoli collegati e fornisce una breve descrizione.

Tipo di accesso	Ruoli collegato	Descrizione
Amministrazione	■ Amministratore (impostazione predefinita) ■ Amministratore della configurazione ■ Dipendente ■ Analista di livello 2 ■ Amministratore Service Desk ■ Amministratore del sistema ■ Amministratore titolari	Fornisce il massimo livello di accesso di protezione a tutti i ruoli di amministrazione chiave. Utilizzato durante l'implementazione e le continue attività di amministrazione. **Nota:** il tipo di accesso Amministrazione è preconfigurato per consentire agli amministratori di passare a uno qualsiasi dei ruoli collegati. Ad esempio, per accedere a una diversa visualizzazione del sistema, gli amministratori possono passare al ruolo Dipendente senza dover uscire dal sistema e accedere nuovamente.
Cliente	■ Cliente	Fornisce accesso altamente ristretto ai clienti *esterni* che utilizzano la visualizzazione self-service.
Dipendente	■ Dipendente	Fornisce accesso altamente ristretto ai clienti *interni* che utilizzano la visualizzazione self-service. Utilizzato per creare pagine relative a nuovi incidenti e all'aggiornamento di incidenti.
Staff IT	■ Analista della configurazione ■ Dipendente ■ Analista di livello 2 (impostazione predefinita) ■ Analista della conoscenza ■ Amministratore Gestione della conoscenza ■ Gestione della conoscenza	Fornisce accesso per operazioni normalmente svolte da analisti agli utenti che lavorano nella propria organizzazione IT ma non fanno parte del team di assistenza. Questo accesso è pensato appositamente per gli utenti che hanno bisogno di accedere a Gestione della conoscenza.

Tipo di accesso	Ruoli collegato	Descrizione
Gestione della conoscenza	■ Amministratore della configurazione ■ Analista della configurazione ■ Visualizzatore della configurazione ■ Dipendente ■ Analista della conoscenza ■ Amministratore Gestione della conoscenza (impostazione predefinita) ■ Gestione della conoscenza ■ Analista di livello 2	Fornisce accesso amministrativo adatto agli utenti che amministrano le funzionalità di Gestione della conoscenza.
Gestione processi	■ Gestione Cambiamento ■ Analista della configurazione ■ Dipendente ■ Gestione incidente (predefinito) ■ Analista di livello 2 ■ Gestione problemi ■ Gestione Service Desk	Fornisce accesso adatto agli utenti che ricoprono ruoli di gestione dei processi chiave.
Gestione Service Desk	■ Gestione servizio clienti ■ Analista della configurazione ■ Dipendente ■ Analista di livello 1 ■ Analista di livello 2 ■ Gestione Service Desk (impostazione predefinita)	Fornisce accesso adatto agli utenti che gestiscono l'assistenza IT o funzioni di assistenza per clienti esterni (tipicamente i supervisori dell'assistenza primaria).

Tipo di accesso	Ruoli collegato	Descrizione
Staff Service Desk	■ Analista della configurazione ■ Visualizzatore della configurazione ■ Rappresentante del servizio clienti ■ Dipendente ■ Analista di livello 1 (impostazione predefinita) ■ Analista di livello 2	Fornisce accesso adatto agli utenti che eseguono attività di assistenza. L'accesso è incentrato sugli utenti che forniscono assistenza primaria.
Amministrazione Support Automation	■ Amministratore automazione supporto	Fornisce accesso agli utenti che si occupano dell'amministrazione di Support Automation.
Analista automazione supporto	■ Analista automazione supporto	Fornisce accesso agli utenti che offrono assistenza in tempo reale agli utenti finali.
Staff dei vendor	■ Analista vendor	Fornisce accesso altamente ristretto ai vendor esterni che si occupano solo di elementi direttamente correlati al proprio prodotto (ad esempio una specifica marca di hardware).

Record ruolo

È possibile assegnare dei ruoli a un tipo di accesso o direttamente a un record contatto di un utente. Se si verifica un conflitto nell'assegnazione dei ruoli, hanno precedenza le assegnazioni dei ruoli dei contatti.

Ogni record ruolo deve essere configurato con i seguenti componenti:

- Un gruppo moduli
- Un tipo di interfaccia utente
- Impostazioni di accesso funzioni
- Una o più schede
- Un set di file della Guida

I seguenti componenti opzionali possono inoltre contribuire alla definizione di ciascun ruolo:

- Strutture menu
- Contatori
- Barre dei menu

- Barre degli strumenti
- Una partizione dati
- Accesso Gestione della conoscenza
- Livello di accesso Support Automation
- Moduli Web di report
- Risorse di accesso rapido

Aree di accesso funzionale

Le aree di accesso funzionale definiscono l'accesso di livello ruolo ai record dei ticket e altri componenti di sistema. La tabella usp_functional_access_type definisce l'area e le tabelle usp_functional_access_level descrivono l'accesso utente.

La seguente tabella mostra le aree di accesso funzionale predefinite:

Nome	Nome codice	Nuovo
Amministrazione	amministrazione	No
Incidente/Problema/Richiesta	call_mgr	No
Ordine di cambiamento	change_mgr	No
Inventario	inventario	No
Issue	issue_mgr	No
Documento della conoscenza	kd	No
Notifica	notifica	No
Riferimento	riferimento	No
Protezione	protezione	No
Annuncio	annuncio	Sì
Riferimento Incidente/Problema/Richiesta	call_mgr_reference	Sì
Modello Incidente/Problema/Richiesta	call_mgr_template	Sì
Modello Ordine di cambiamento	change_mgr_template	Sì
Riferimento Ordine di cambiamento	change_reference	Sì
Elemento della configurazione	ci	Sì
Elemento della configurazione comune di sola lettura	ci_common_ro	Sì
Riferimento elemento di configurazione	ci_reference	Sì
Contatto	contatto	Sì

Gruppo	gruppo	Sì
Modello Issue	issue_mgr_template	Sì
Riferimento Issue	issue_reference	Sì
Posizione	ubicazione	Sì
Amministrazione sito multiplo	multisite_admin	Sì
Riferimento sito multiplo	multisite_reference	Sì
Riferimento notifica	notification_reference	Sì
Organizzazione	organization	Sì
Prioritizzazione	prioritizzazione	Sì
Livello di servizio	service_level	Sì
Sito	sito	Sì
Query memorizzata	stored_queries	Sì
Support Automation	sa	Sì
Indagine	indagine	Sì
Amministratore titolare	tenant_admin	Sì
Fuso orario	timezone	Sì
Riferimento flusso di lavoro	workflow_reference	Sì
Turno	turni	Sì

Modalità di aggiunta di un'area di accesso funzionale

Quando si aggiunge un'area di accesso funzionale, i ruoli esistenti dispongono automaticamente dell'accesso Modifica. È possibile rivedere e modificare i livelli di accesso per concedere le autorizzazioni appropriate.

Per aggiungere un'area di accesso funzionale, procedere come segue:

1. Nella scheda Amministrazione, selezionare Gestione protezione e ruoli, Accesso funzionale.
2. Fare clic su Crea Nuovo.

   Viene visualizzata la pagina di elenco Crea Nuovo accesso funzionale
3. Compilare i campi dell'area di accesso funzionale secondo necessità.
4. Fare clic su Salva.

   Viene visualizzata la pagina Dettagli accesso funzionale.

5. Applicare livelli di accesso a uno (a pagina 362) o più (a pagina 360) ruoli.

Nota: per istruzioni dettagliate sulle aree di accesso funzionale, consultare la *Guida in linea*.

Applicazione di livelli di accesso a più ruoli

Per un'area di accesso funzionale, è possibile impostare i livelli di accesso per ogni ruolo per risparmiare tempo. Anziché utilizzare Gestione ruoli, si aggiorna l'area di accesso funzionale con i livelli di accesso dei ruoli appropriati.

Per applicare livelli di accesso a più ruoli, procedere come segue:

1. Nella scheda Amministrazione, selezionare Gestione protezione e ruoli, Accesso funzionale.
2. Fare clic sul nome dell'area funzionale.
3. Nella scheda Ruoli fare clic su Modifica in elenco.
4. Rivedere e aggiornare ogni ruolo in base alle esigenze. Sono disponibili i seguenti livelli di accesso:

   Nessuno

   Nega al ruolo l'accesso all'oggetto di funzione.

   Visualizza

   Concede funzionalità di sola lettura per l'oggetto di funzione.

   Modifica

   Concede accesso in scrittura e lettura per l'oggetto di funzione.
5. Continuare a selezionare ruoli e a scegliere livelli di accesso.
6. (Facoltativo) Fare clic su Modifica tutto.
7. Fare clic su Salva.

   Le modifiche apportate ai ruoli vengono applicate immediatamente.

Nota: per informazioni su ruoli e livelli di accesso funzionale, consultare la *Guida in linea.*

Esempio: modifica dei livelli di accesso per l'area di accesso funzionale Annuncio

L'esempio riportato di seguito illustra la modifica dei livelli di accesso per l'area di accesso funzionale Annuncio.

1. Nella scheda Amministrazione, selezionare Gestione protezione e ruoli, Accesso funzionale.

   Viene visualizzata la pagina Dettagli accesso funzionale.

2. Fare clic su Annuncio.
3. Nella scheda Ruoli fare clic su Modifica in elenco.
4. Selezionare Analista di livello 2.
5. Selezionare Visualizza da Livello di accesso.

   Il livello di accesso del ruolo Analista di livello 2 viene evidenziato con il valore di Visualizza.
6. Selezionare Analista della configurazione.
7. Selezionare Modifica da Livello di accesso.

   Il livello di accesso del ruolo Analista della configurazione viene evidenziato con il valore di Modifica.
8. Fare clic su Salva.

   Un messaggio conferma la modifica.
9. Accedere con ruolo di Analista di livello 2.
10. Selezionare la visualizzazione degli annunci.

    Viene visualizzata la pagina Annunci.
11. Fare clic su un annuncio.

    Viene visualizzato un messaggio che ricorda che un Analista di livello 2 può solo visualizzare gli annunci.
12. Impostare il ruolo su Analista della configurazione.
13. Selezionare la visualizzazione degli annunci.

    Viene visualizzata la pagina Annunci.
14. Fare clic su un annuncio.

    Viene visualizzata la pagina Aggiorna annuncio. In qualità di Analista della configurazione, l'utente può modificare gli annunci.

Applicazione di un livello di accesso a un ruolo

È possibile utilizzare Gestione ruoli per modificare la modalità con cui gli utenti accedono all'interfaccia utente. Quando si modificano i livelli di accesso per un ruolo, nell'interfaccia utente vengono visualizzati solo gli oggetti, le pagine e le voci di menu consentiti in base al livello di accesso. Ad esempio, se un ruolo non può più creare contatti, nel menu File non viene visualizzata la voce Nuovi contatti.

Per applicare un livello di accesso a un ruolo, procedere come segue:

1. Nella scheda Amministrazione, fare clic su Gestione protezione e ruoli, Gestione ruoli e quindi su Elenco ruoli.
2. Nell'Elenco ruoli, fare clic con il pulsante destro del mouse sul nome del ruolo e selezionare Modifica dal menu di scelta rapida.
3. Fare clic su Modifica in elenco nella scheda Accesso funzioni.
4. Fare clic su un nome di funzione.

   La riga viene evidenziata.
5. Aggiornare le aree di accesso funzionale con i seguenti livelli di accesso secondo necessità:

   Nessuno

   Nega al ruolo l'accesso all'oggetto di funzione.

   Visualizza

   Concede funzionalità di sola lettura per l'oggetto di funzione.

   Modifica

   Concede accesso in scrittura e lettura per l'oggetto di funzione.
6. Fare clic su Salva.

   Un messaggio conferma la modifica. Il ruolo può utilizzare immediatamente l'area di accesso funzionale al livello di accesso specificato.
7. Verificare il livello di accesso accedendo con il ruolo e verificando menu, opzioni di pagina e pulsanti.

Esempio: concessione dell'accesso Modifica al ruolo Analista di livello 2 per i ticket

L'esempio seguente illustra come cambia l'interfaccia utente quando si concede a un ruolo Analista di livello 2 l'accesso per modificare i ticket.

1. Nella scheda Amministrazione, fare clic su Gestione protezione e ruoli, Gestione ruoli e quindi su Elenco ruoli.

   Viene visualizzato l'Elenco ruoli.
2. Fare clic con il pulsante destro del mouse su Analista di livello 2 e selezionare Modifica dal menu di scelta rapida.

3. Fare clic su Modifica in elenco nella scheda Accesso funzioni.
4. Selezionare Riferimento incidente/problema/richiesta.
5. Selezionare Modifica da Livello di accesso.

   Il livello di accesso viene aggiornato su Modifica.
6. Fare clic su Salva e disconnettersi.

   Un messaggio conferma la modifica.
7. Accedere con ruolo di Analista di livello 2.
8. Selezionare Cerca, Incidenti.
9. Fare clic su Cerca e aprire un incidente.

   Nella pagina Dettagli incidente è visualizzato il pulsante Modifica in elenco. In qualità di Analista di livello 2, è possibile modificare il ticket.

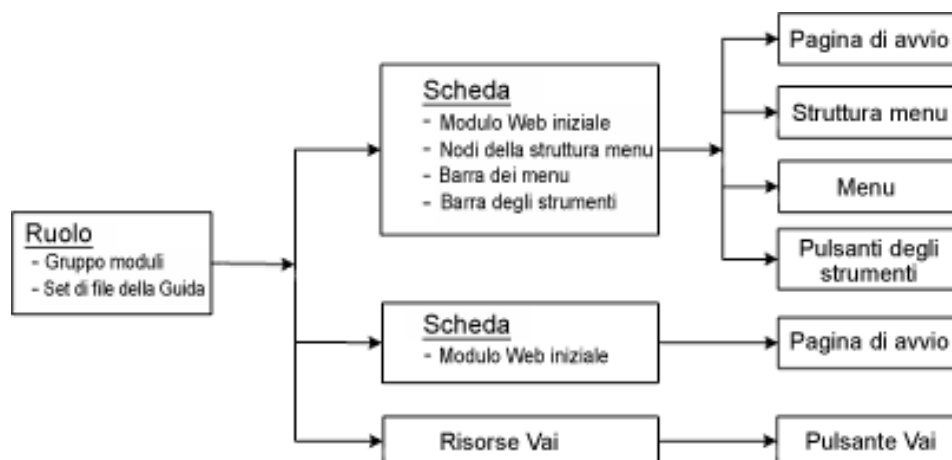
Partizioni dati

Le partizioni dati sono sottoinsiemi del database di CA SDM che consentono di controllare l'accesso a livello di record. È possibile associare una partizione dati a un ruolo per controllare l'accesso ai ticket e ad altri record tramite l'interfaccia Web.

Per ulteriori informazioni sull'utilizzo delle partizioni dati, consultare Associazioni di partizioni dati (a pagina 298).

Navigazione basata su ruoli

Ogni visualizzazione dell'interfaccia Web da parte dell'utente è definita da un ruolo. Gli utenti a cui sono assegnati più ruoli possono passare da una visualizzazione a un'altra.

Lo schema seguente mostra le relazioni tra ruoli e altri oggetti per offrire una presentazione dell'interfaccia Web basata su ruoli.

Schede

Una scheda è un'entità grafica visualizzata, collegata ad un ruolo al fine di presentare le funzioni agli utenti con quel ruolo. Quando un utente accede al sistema, la finestra principale mostra le schede assegnate al ruolo predefinito dell'utente.

Le schede definiscono le suddivisioni più importanti nell'interfaccia Web della finestra principale. Ogni scheda è configurata in modo da mostrare una serie appropriata di funzionalità dell'interfaccia utente al ruolo o ai ruoli che la utilizzano.

Tutti i ruoli devono disporre di almeno una scheda. È possibile associare una o più schede a un ruolo. Ogni scheda ha un numero di sequenza che ne determina l'ordine di visualizzazione nella finestra principale. Se ad un ruolo è associata una sola scheda, viene visualizzata la pagina di avvio e non la scheda.

È possibile configurare le schede in modo che contengano le seguenti funzionalità di visualizzazione:

- Una pagina di avvio (il modulo Web predefinito), visualizzata quando un utente seleziona la scheda. La pagina di avvio è un elemento obbligatorio di tutte le schede. Si può assegnare una sola pagina di avvio a ogni scheda.

  Nota: è possibile configurare un pagina di avvio in modo che visualizzi report grafici di BusinessObjects, affinché gli utenti possano generare i report al momento dell'esecuzione. Per ulteriori informazioni, consultare il capitolo relativo al reporting di CA Business Intelligence (a pagina 861).

- Una barra dei menu, che mostra elenchi a discesa di comandi, ad esempio File, Visualizza e Cerca. La barra dei menu è opzionale. Si può assegnare una sola barra dei menu a ogni scheda.
- Una barra degli strumenti, che mostra pulsanti degli strumenti per accedere facilmente ai comandi di menu più utilizzati. La barra degli strumenti è facoltativa.

CA SDM fornisce diverse schede predefinite. È possibile assegnare schede predefinite a un ruolo, modificarle e creare schede personalizzate.

Importante. Assegnare il numero di schede consentito dalla finestra del browser. Se il numero di schede assegnato è superiore, le schede con numeri di sequenza superiori si estenderanno oltre l'area visualizzabile della finestra e non saranno accessibili all'utente.

Importante. Includere solo le schede che contengono moduli che si trovano nel gruppo assegnato al ruolo creato o modificato. Non assegnare ad esempio la scheda Cliente o Dipendente al ruolo Amministratore, in quanto si verificherebbe un errore se gli utenti tentano di accedervi. Il gruppo di moduli del ruolo è specificato nel campo Personalizzazione gruppo moduli della pagina Dettagli ruolo e viene visualizzato anche nella colonna Gruppo di moduli nella pagina Elenco ruoli. Per un elenco dei moduli Web inclusi in ogni gruppo di moduli, consultare la sezione Gruppi di moduli (a pagina 1223).

Schede predefinite

Nella seguente tabella vengono mostrate le schede predefinite assegnate ad ogni ruolo. Le schede sono elencate in ordine di sequenza. Ne viene inoltre indicata la posizione da sinistra a destra nella finestra.

Nota: in diversi casi sono presenti più versioni delle schede con lo stesso nome visualizzato. La scheda Service Desk per il ruolo Amministratore fornisce ad esempio accesso completo alle funzionalità di CA SDM, mentre la scheda Service Desk per il ruolo Gestione cambiamento pone maggiore attenzione sugli ordini di cambiamento.

Ruolo	Schede
Amministratore	■ Scheda Service Desk con contatore e menu completo ■ scheda Conoscenza ■ Scheda Amministrazione con struttura menu completa ■ Scheda Report - Amministratore ■ Scheda Modifica calendario ■ Scheda CA CMDB ■ Scheda Support Automation

Ruolo	Schede
Gestione Cambiamento	■ Scheda Report - Gestione Cambiamento ■ Scheda Service Desk - Gestione Cambiamento ■ Scheda Modifica calendario
Amministratore della configurazione	■ Scheda CA CMDB ■ Scheda Amministrazione - Amministratore della configurazione
Analista della configurazione	■ Contatore CA CMDB - Analista della configurazione
Visualizzatore della configurazione	■ Contatore CA CMDB - Visualizzatore della configurazione
Cliente	■ Scheda Cliente
Gestione servizio clienti	■ Scheda Service Desk - Gestione servizio clienti ■ scheda Conoscenza ■ Scheda Report - Gestione servizio clienti
Rappresentante del servizio clienti	■ Scheda Service Desk - Rappresentante del servizio clienti ■ Scheda Profilo rapido ■ scheda Conoscenza
Dipendente	■ Scheda Dipendente
Gestione Incidente	■ Scheda report - Gestione incidente ■ Scheda Service Desk - Gestione incidente ■ scheda Conoscenza
Analista della conoscenza	■ Scheda Service Desk - Analista della conoscenza ■ scheda Conoscenza ■ Pianificazione Gestione della conoscenza ■ Scheda Scheda Report della conoscenza ■ Scheda Report - Analista della conoscenza
Gestione della conoscenza	■ Scheda Service Desk - Gestione della conoscenza ■ scheda Conoscenza ■ Pianificazione Gestione della conoscenza ■ Scheda Amministrazione - Gestione della conoscenza ■ Scheda Scheda Report della conoscenza ■ Scheda Report - Gestione della conoscenza
Amministratore Gestione della conoscenza	■ Scheda amministrazione - Amministratore della conoscenza

Ruolo	Schede
Analista di livello 1	■ Scheda Service Desk - Analista di livello 1 ■ Scheda Profilo rapido ■ scheda Conoscenza
Analista di livello 2	■ Scheda Service Desk - Analista di livello 2 ■ scheda Conoscenza ■ Scheda Modifica calendario
Gestione problemi	■ Scheda Report - Gestione Problema ■ Scheda Service Desk - Gestione problemi ■ scheda Conoscenza
Amministratore Service Desk	■ Scheda Amministrazione - Amministratore Service Desk
Gestione Service Desk	■ Scheda Report - Gestione Service Desk ■ Scheda Service Desk - Gestione Service Desk ■ scheda Conoscenza ■ Scheda Modifica calendario
Amministratore automazione supporto	■ Scheda Service Desk - Analista di livello 1 ■ Scheda Support Automation ■ Amministrazione Support Automation ■ Scheda Profilo rapido ■ scheda Conoscenza
Analista automazione supporto	■ Scheda Service Desk - Analista di livello 1 ■ Scheda Support Automation ■ Scheda Profilo rapido ■ scheda Conoscenza
Amministratore del sistema	■ Scheda Amministrazione - Amministratore di sistema
Amministratore titolari	■ Scheda Amministrazione - Amministratore titolari
Analista vendor	■ Scheda Service Desk - Analista vendor

Moduli Web

I moduli Web definiscono le pagine visualizzate nell'interfaccia Web CA SDM.

Sono disponibili quattro tipi di modulo Web:

- URL di report BusinessObjects
- HTMPL, pagina
- Risorsa di accesso rapido
- Personalizzato (ad esempio un URL per una pagina Web di terze parti)

Per informazioni sulla creazione di moduli Web personalizzati, consultare la sezione Creazione di un record di modulo Web (a pagina 378).

Gruppi moduli

I gruppi di moduli definiscono i set di pagine dell'interfaccia Web di CA SDM disponibili per un ruolo. Ciascun ruolo può presentare un gruppo di moduli. Gli utenti possono visualizzare soltanto le pagine Web contenute nel gruppo di moduli assegnato al proprio ruolo.

Ad ogni tipo di interfaccia è associato un gruppo di moduli, ovvero un set di file HTMPL che definiscono le pagine che possono essere visualizzate con il tipo di interfaccia in oggetto.

CA SDM fornisce i seguenti gruppi di moduli predefiniti:

- Analista
- Cliente
- Dipendente
- ITIL

È possibile utilizzare i gruppi di moduli predefiniti nella relativa configurazione predefinita, modificare i gruppi di moduli predefiniti e creare gruppi di moduli nuovi utilizzando Web Screen Painter. È possibile visualizzare un elenco dei nomi file HTMPL inclusi in ogni gruppo di moduli (a pagina 1223) predefinito.

Strutture menu

Le strutture menu sono elenchi gerarchici di nodi (risorse struttura menu) visualizzati nel riquadro di navigazione sul lato sinistro della finestra principale dell'interfaccia Web.

Un ruolo può presentare una struttura menu, che fornisce i nodi per accedere a diverse aree funzionali del sistema. Il ruolo Amministratore predefinito presenta ad esempio una struttura menu che include i nodi per le funzioni di amministrazione dei ruoli e dei sistemi, le funzioni di amministrazione di Service Desk e diverse altre.

Una struttura menu rende disponibile, ai ruoli che la includono, un gruppo specifico di risorse che consentono di accedere alle aree funzionali del sistema.

In CA SDM sono disponibili strutture menu predefinite per i seguenti ruoli:

- Amministratore (admin_tree)
- Amministratore CA CMDB (cmdb_adm_tree)
- Amministratore Gestione della conoscenza (kt_adm_tree)
- Gestione della conoscenza (kt_mgr_tree)
- Amministratore Support Automation (sa_admin_tree)
- Amministratore Service Desk (sd_adm_tree)
- Amministratore di sistema (sys_adm_tree)
- Amministratore titolari (tn_admin_tree)

È possibile modificare i campi Nome, Stato record e Descrizione dei record delle strutture menu, ma non è possibile personalizzarli aggiungendo o rimuovendo le relative risorse delle strutture menu.

Per creare una struttura menu personalizzata, si può creare un nuovo record di struttura menu oppure copiare e personalizzare una delle strutture menu predefinite.

Nota: il campo non modificabile Interno, presente in ogni record di struttura menu, indica se la struttura menu può essere personalizzata. Se il valore del campo è SÌ, la struttura menu è predefinita e non può essere personalizzata. Se invece il valore è NO, la struttura menu è definita a livello di sito e può essere personalizzata. Il pulsante Personalizza menu viene visualizzato solo sui record dei dettagli della struttura menu che presentano il valore NO nel campo Interno.

Una struttura menu, dopo essere stata associata a una scheda, sarà disponibile per tutti i ruoli che possono accedere alla scheda.

Risorse struttura menu

Le risorse di una struttura menu definiscono gli elementi cui gli utenti possono accedere dalla struttura menu.

Una risorsa struttura menu è composta da un nome, una descrizione e un frammento di URL oppure dal nome del file HTMPL utilizzato dal motore Web che controlla la pagina Web visualizzata.

Barre dei menu

La barra dei menu è un elemento dell'interfaccia utente che visualizza un elenco orizzontale dei menu nella finestra principale dell'interfaccia Web. Ogni menu contiene un elenco a discesa delle opzioni e dei comandi. È possibile definire barre dei menu personalizzate per tutti i ruoli che possono essere creati.

I record della barra dei menu specificano il modulo HTMPL che controlla le voci di menu cui è possibile accedere dalla barra.

Nota: per definire la funzionalità della barra dei menu, occorre utilizzare l'applicazione Web Screen Painter. Per informazioni su come configurare la funzionalità di una barra dei menu predefinita o personalizzata, vedere la *Guida in linea di Web Screen Painter*.

Nella seguente tabella sono elencate le barre dei menu predefinite e le schede in cui vengono utilizzate.

Barra dei menu	Schede associate
Amministrazione	■ Scheda Amministrazione - Amministratore della configurazione ■ Scheda amministrazione - Amministratore della conoscenza ■ Scheda Amministrazione - Gestione della conoscenza ■ Scheda Amministrazione - Amministratore Service Desk ■ Scheda Amministrazione - Amministratore di sistema ■ Scheda Amministrazione - Amministratore titolari ■ Scheda Amministrazione con struttura menu completa
CA CMDB	■ Scheda CA CMDB con contatore e menu completo
Calendario dei Cambiamenti	■ Scheda Modifica calendario
Conoscenza	■ scheda Conoscenza ■ Pianificazione Gestione della conoscenza
Service Desk	■ Scheda Service Desk con contatore e menu completo
Service Desk - Gestione Cambiamento	■ Scheda Service Desk - Gestione Cambiamento
Service Desk - Gestione del servizio clienti	■ Scheda Service Desk - Gestione servizio clienti
Service Desk - Rappresentante del servizio clienti	■ Scheda Service Desk - Rappresentante del servizio clienti
Service Desk - Gestione incidente	■ Scheda Service Desk - Gestione incidente
Service Desk - Analista della conoscenza	■ Scheda Service Desk - Analista della conoscenza

Barra dei menu	Schede associate
Service Desk - Gestione della conoscenza	■ Scheda Service Desk - Gestione della conoscenza
Service Desk - Analista di livello 1	■ Scheda Service Desk - Analista di livello 1
Service Desk - Analista di livello 2	■ Scheda Service Desk - Analista di livello 2
Service Desk - Gestione Problema	■ Scheda Service Desk - Gestione problemi
Service Desk - Gestione Service Desk	■ Scheda Service Desk - Gestione Service Desk
Service Desk - Analista vendor	■ Scheda Service Desk - Analista vendor
Support Automation - Analista	■ Scheda Support Automation - Analista Support Automation

Barre degli strumenti

Le barre degli strumenti estendono la funzionalità delle barre dei menu aggiungendo le funzioni che consentono di visualizzare uno o più pulsanti degli strumenti a destra del menu.

I pulsanti degli strumenti vengono visualizzati come icone sulla barra degli strumenti. Facendo clic sul pulsante di uno strumento è possibile accedere ai comandi o alle opzioni di menu utilizzati più di frequente.

Nota: l'applicazione Web Screen Painter consente di definire la funzionalità della barra degli strumenti. Per informazioni su come configurare la funzionalità di una barra degli strumenti predefinita o personalizzata, vedere la *Guida in linea di Web Screen Painter*.

Risorse di accesso rapido

Il pulsante *Vai* consente di trovare facilmente un determinato record.

Le risorse di accesso rapido sono un tipo di modulo Web. Se un ruolo presenta risorse di accesso rapido, quando un utente accede con tale ruolo, il pulsante Vai viene visualizzato nell'angolo superiore destro della finestra principale di CA SDM e in tutte le finestre popup. Al pulsante Vai sono associati due campi nell'interfaccia utente:

- Un elenco a discesa per selezionare il tipo di record da cercare (ad esempio un ordine di cambiamento)
- Una casella di testo per immettere un valore al fine di identificare un determinato record (ad esempio 135 per trovare l'ordine di cambiamento 135)

L'assegnazione delle risorse di accesso rapido ad un ruolo consente di specificare i tipi di record che gli utenti con quel ruolo possono cercare. Il ruolo Amministratore predefinito presenta ad esempio le seguenti risorse di accesso rapido:

- Ordine di cambiamento
- Documento per ID
- Incidente
- Issue
- Conoscenza
- Problema
- Richiesta
- Utente per ID
- Utente per nome
- Utente per n. telefono

Set di file della Guida

I set di file della Guida sono raccolte di argomenti della guida in linea disponibili per gli utenti, a seconda del ruolo assegnato e impostato. Se si accede con il ruolo di amministratore, ad esempio, si possono visualizzare gli argomenti della guida in linea contenuti nel set di file della Guida per gli amministratori. Se si passa al ruolo Dipendente, verrà visualizzato il set di file della Guida per i dipendenti.

A ogni ruolo predefinito corrisponde un set di file della Guida. Si possono creare set di file della Guida in linea personalizzati per qualsiasi ruolo.

Nota: per informazioni sull'utilizzo delle definizioni di set di file della Guida, vedere la *Guida in linea*.

Modalità di implementazione di un ruolo personalizzato

I ruoli predefiniti sono sufficienti per diversi siti. In alcuni casi è tuttavia possibile che sia necessario creare un ruolo personalizzato che soddisfi le esigenze aziendali specifiche del sito all'interno dell'organizzazione.

Nel seguente processo vengono evidenziate le attività necessarie per l'implementazione di un nuovo ruolo. Nell'esempio riportato viene illustrato come sia possibile implementare un ruolo per un gruppo ridotto di analisti incaricati dell'esame e dell'autorizzazione dei ticket ordine di cambiamento.

Per implementare un ruolo personalizzato, eseguire le attività illustrate nel seguente esempio:

1. Creare un nuovo record ruolo utilizzando i seguenti valori di campo:

   Nome ruolo

   Analista modifiche

   Codice

   chg_anal

   Personalizzazione gruppo moduli

   Analista

   Documento preferito

   Incidente

2. Selezionare Analista Service Desk nel campo Partizione dati della scheda Autorizzazione.

3. Selezionare Modifica nel campo Ordini di cambiamento nella scheda Accesso funzioni.

4. Immettere i seguenti valori nella scheda Interfaccia Web:

   Tipo interfaccia utente Web

   Analista

   Visualizzazione guida

   Analista modifiche

5. Selezionare le seguenti schede:

   - Scheda Report - Analista modifiche
   - Scheda Service Desk - Analista modifiche
   - Scheda Modifica calendario

6. Selezionare i seguenti report nella scheda Moduli Web di report:

   - Durata ordini di cambiamento attivi per priorità per stato
   - Ordini di cambiamento attivi nei fine settimana
   - Ordini di cambiamento per tipo di servizio con errori per categorie cambiamento

7. Aggiungere la risorsa ordine di cambiamento nella scheda Risorse di accesso rapido.

8. Creare un set di file della Guida denominato Analista modifiche che includa tutto il contenuto appropriato per il nuovo ruolo.

   Per ulteriori informazioni, consultare la sezione Creazione e pubblicazione di un set di file della Guida (a pagina 381).

9. Creare le seguenti schede personalizzate utilizzando le funzioni appropriate per il nuovo ruolo:
   - Scheda Report - Analista modifiche
   - Scheda Service Desk - Analista modifiche
10. Creare una struttura menu personalizzata che includa tutti i nodi appropriati per il nuovo ruolo.

    Per ulteriori informazioni, vedere Modalità di implementazione di una struttura menu personalizzata (a pagina 374).

Modalità di implementazione di una struttura menu personalizzata

Per molti siti, la struttura menu predefinita è sufficiente. Tuttavia, possono verificarsi situazioni in cui si desidera personalizzare un ruolo implementando una specifica struttura menu.

In molti casi è più facile iniziare con una copia della struttura menu predefinita per poi aggiungere, rimuovere o riorganizzare i nodi all'interno della gerarchia. In alternativa, si può creare una struttura menu e costruire una gerarchia di nodi completamente nuova.

Per rendere una struttura menu disponibile per un ruolo, è possibile procedere in uno dei seguenti modi:

- Sostituire la struttura menu nel modulo Web (Pagina di avvio) per la scheda che visualizza la struttura admin_tree originale.
- Creare un nuovo modulo Web, quindi associarlo, insieme alla struttura menu, a una scheda.

Per implementare un menu personalizzato, procedere come segue:

1. Copiare una delle strutture menu predefinite.

   Nota: prendere nota del valore immesso nel campo Codice.
2. Creare un modulo Web utilizzando i seguenti valori di campo:
   - **Tipo:** HTMPL
   - **Risorsa:**

     `$cgi?SID=$SESSION.SID+FID=123+OP=DISPLAY_FORM+HTMPL=admin_main_role.htmpl +KEEP.tree_code=`*`menu_tree_code`*

     Nota: specificare il valore del codice per la struttura menu creata al passaggio 1 per menu_tree_code. Il codice admin_main_role.htmpl utilizza il valore della variabile KEEP.tree_code come struttura menu.

3. Creare un record scheda utilizzando i seguenti valori di campo:
   - **Pagina di avvio:** il modulo Web creato nel passaggio 2
   - **Barra dei menu:** Amministrazione

   Nota: Amministrazione è una barra di menu generica utilizzata da diversi ruoli, pertanto non è relativa a ruoli specifici.
4. Assegnare la scheda creata nel passaggio 3 al ruolo a cui si desidera fornire accesso alla struttura menu personalizzata.
5. Uscire da CA SDM e accedervi di nuovo.

   Nella scheda Amministrazione viene visualizzata la struttura menu personalizzata.

Ulteriori informazioni:

Creazione di record di modulo Web (a pagina 378)

Creazione di un record ruolo

Gli amministratori possono creare ruoli personalizzati per soddisfare i requisiti aziendali specifici di determinati siti.

Per creare un ruolo

1. Selezionare Gestione protezione e ruoli, Gestione ruoli, Elenco Ruoli, nella scheda Amministrazione.

   Viene visualizzata la pagina Elenco ruoli.
2. Fare clic su Crea Nuovo.

   Viene visualizzata la pagina Crea nuovo ruolo.
3. Inserire i dati nei seguenti campi:

   Nome ruolo

   Specifica il nome che identifica il ruolo all'interno di tutta l'interfaccia utente.

   Codice

   Specifica il codice che identifica il ruolo nel sistema.

   Nota: una volta salvato il record, questo campo non può essere modificato.

   Stato record

   Indica se il ruolo è attivo o non attivo.

   Predefinito?

   Indica se questo è il ruolo predefinito.

Personalizzazione gruppo moduli

Specifica un gruppo di moduli predefinito o personalizzato.

Documento preferito

Specifica il documento utilizzato dal ruolo per immettere i ticket nel sistema.

Descrizione

Descrive lo scopo del ruolo. Questa descrizione compare nella pagina Elenco ruoli e può facilitare l'assegnazione degli utenti ai ruoli adeguati.

Fare clic su Salva.

La definizione del ruolo viene salvata e compare la pagina Dettagli ruolo.

Creazione di un record scheda

È possibile creare schede personalizzate da visualizzare nella pagina principale dell'interfaccia Web. Quando lo si collega a un record ruolo, un record scheda diviene disponibile per gli utenti assegnati a tale ruolo.

Per creare una scheda

1. Selezionare Gestione ruoli e protezione, Gestione ruoli, Schede nella scheda Amministrazione.

   Viene visualizzata la pagina Elenco schede.

2. Fare clic su Crea Nuovo.

   Viene visualizzata la pagina Crea nuova scheda.

3. Inserire i dati nei seguenti campi:

   Nome scheda

   Specifica il nome che identifica la scheda all'interno dell'interfaccia amministrativa. Ad esempio, il nome della scheda compare alla pagina Elenco Schede.

   Codice

   Specifica il codice che identifica la scheda nel sistema.

   Nota: il codice, una volta definito, non può essere modificato.

   Stato record

   Indica se la scheda è attiva o non attiva.

   Nome visualizzato

   Specifica il nome visualizzato nella rappresentazione grafica della scheda nell'interfaccia utente.

Pagina di avvio

Specifica il modulo Web iniziale che viene visualizzato nella finestra principale se un utente seleziona questa scheda.

Importante. la pagina di avvio e la barra dei menu devono appartenere allo stesso gruppo di moduli. Se si definisce una scheda con una pagina di avvio e una barra dei menu che appartengono a gruppi di moduli (a pagina 1223) diversi, si verifica un errore quando gli utenti accedono alla scheda.

Barra dei menu

Specifica la barra dei menu che compare nella finestra principale se un utente seleziona questa scheda.

Fare clic su Salva.

La scheda è stata creata.

Creazione di un record barra dei menu

Si possono creare barre dei menu personalizzate per controllare l'accesso alle funzionalità del sistema per i ruoli definiti dall'utente.

Per creare una barra dei menu

1. Selezionare Gestione ruoli e protezione, Gestione ruoli, Barre dei menu nella scheda Amministrazione.

   Viene visualizzata la pagina Elenco barra dei menu.

2. Fare clic su Crea Nuovo.

   Viene visualizzata la pagina Crea nuova barra dei menu.

3. Inserire i dati nei seguenti campi:

   Nome barra dei menu

   (Obbligatorio) Specifica il nome che identifica la barra dei menu. Utilizzare questo campo per chiarire la funzionalità disponibile dalla barra dei menu.

   Codice

   (Obbligatorio) Specifica il codice che identifica la barra dei menu nel prodotto. Il codice, una volta definito, non può essere modificato.

   Stato record

   Indica se la barra dei menu è attiva o non attiva.

   Nome HTMPL

   Specifica il nome del modulo HTMPL che contiene la definizione della barra dei menu. La barra dei menu è sviluppata mediante Web Screen Painter.

Descrizione

Descrive la barra dei menu. È utile per identificare ulteriormente la barra dei menu e i ruoli che la utilizzano.

Fare clic su Salva.

La definizione della barra dei menu viene salvata e compare la pagina Dettagli barra dei menu.

Creazione di record di modulo Web

Gli amministratori possono creare moduli Web personalizzati che fungono da pagine di avvio per le schede, report da visualizzare sulle schede, risorse "Vai" o un altro URL.

Per creare un modulo Web

1. Selezionare Gestione ruoli e protezione, Gestione ruoli, Moduli Web nella scheda Amministrazione.

   Viene visualizzata la pagina Elenco moduli Web.

2. Fare clic su Crea Nuovo.

   Viene visualizzata la pagina Crea nuovo modulo Web.

3. Inserire i dati nei seguenti campi:

   Nome modulo Web

   (Obbligatorio) Specifica il nome che identifica il modulo Web.

   Stato record

   Indica se il modulo Web è attivo o non attivo.

   Codice

   (Obbligatorio) Specifica il codice che identifica il modulo Web nel sistema. Il codice, una volta definito, non può essere modificato.

   Nota: questo campo specifica il valore web_form_name nella scheda Proprietà per un modulo multiframe di Web Screen Painter.

   Tipo

   Specifica uno dei seguenti tipi di modulo Web che si creano:

   - **Pagina HTMPL**—Consente di visualizzare una pagina Web che funge da pagina iniziale per una delle schede personalizzate che si creano.
   - **Report**—Specifica un report CA SDM che compare in ogni scheda.
   - **Risorsa Vai**—Specifica una risorsa "Pulsante Vai".
   - **Altro**—Consente di accedere a qualsiasi altra pagina Web esterna mediante URL.

Descrizione

Descrive il modulo Web. Questa descrizione consente di identificare ulteriormente il modulo Web, la posizione in cui viene visualizzato e il relativo scopo.

Risorsa

Specifica il codice che richiama il modulo Web. Può essere il codice di riga di comando o un URL.

Esempio: aprire il modulo HTMPL "menu_tab_dflt.htmpl":

```
$cgi?SID=$SESSION.SID+FID=123+OP=DISPLAY_FORM+HTMPL=menu_tab_dflt.htmpl
```

Fare clic su Salva.

Copia di una struttura menu

È possibile copiare una struttura menu esistente da utilizzare come punto di partenza per una struttura menu personalizzata.

Per copiare una struttura menu

1. Selezionare Gestione ruoli e protezione, Gestione ruoli, Strutture menu nella scheda Amministrazione.

   Viene visualizzata la pagina Elenco strutture menu.

2. Fare clic sulla struttura menu da copiare.

   Viene visualizzata la pagina Dettagli struttura menu.

3. Fare clic su File, Copia.

   Viene visualizzata la pagina Crea nuova struttura menu.

4. Inserire i dati nei seguenti campi:

   Nome struttura menu

   (Obbligatorio) Specifica il nome che si assegna per identificare la struttura menu.

   Codice

   (Obbligatorio) Specifica il codice che identifica la struttura menu nel sistema. Il codice, una volta definito, non può essere modificato.

   Stato record

   Indica se la struttura menu è attiva o non attiva.

Descrizione

Descrive la struttura menu. È utile per fornire ulteriori dettagli sulla struttura menu e sui ruoli che la utilizzano.

Fare clic su Salva.

Viene visualizzata la pagina Dettagli struttura menu.

5. Fare clic su Personalizza menu.

   Viene visualizzata una copia della struttura menu originale.

6. Personalizzare la struttura menu in base alle proprie esigenze.

   Nota: per dettagli sull'aggiunta, la rimozione o la modifica di risorse di struttura menu, consultare la *Guida in linea*.

Creazione e personalizzazione di una struttura menu

È possibile creare e personalizzare strutture menu partendo da una delle strutture menu predefinite fornite.

Per creare e personalizzare una struttura menu

1. Selezionare Gestione ruoli e protezione, Gestione ruoli, Strutture menu nella scheda Amministrazione.

   Viene visualizzata la pagina Elenco strutture menu.

2. Fare clic su Crea Nuovo.

   Viene visualizzata la pagina Crea nuova struttura menu.

3. Inserire i dati nei seguenti campi:

   Nome struttura menu

   (Obbligatorio) Il nome che si assegna per identificare la struttura menu.

   Codice

   (Obbligatorio) Il codice che identifica la struttura menu nel sistema. Il codice, una volta definito, non può essere modificato.

   Stato record

   Indica se la struttura menu è attiva o non attiva.

   Descrizione

   Una descrizione della struttura menu. È utile per fornire ulteriori dettagli sulla struttura menu e sui ruoli che la utilizzano.

4. Fare clic su Salva.

5. Fare clic su Personalizza menu.

   Viene visualizzato un modulo che consente di personalizzare la struttura menu. A questo punto la struttura menu contiene solo un nodo di livello superiore, con il testo immesso come nome.

6. Fare clic con il pulsante destro del mouse sulla struttura menu e selezionare Crea Nuovo nodo.

   Viene visualizzata la finestra Crea nuovo nodo.

7. Inserire i dati nei seguenti campi:

   Nome nodo

   Immettere un nome per il nodo. Questo è il nome visualizzato nella struttura menu.

   Descrizione

   Immettere una descrizione per il nodo. È utile per definire ulteriormente lo scopo del nodo.

   Risorsa

   Immettere il nome della risorsa direttamente nel campo o fare clic sull'icona di ricerca per selezionare la risorsa da un elenco. La risorsa struttura menu determina l'azione da eseguire quando l'utente seleziona il nodo dalla struttura menu.

8. Ripetere i passaggi 6 e 7 il numero di volte necessario per creare la serie di nodi che si intende visualizzare nella struttura menu.

   Nota: per maggiori informazioni sull'aggiunta, la rimozione o la modifica di risorse di struttura menu, consultare la *Guida in linea*.

9. Fare clic su Salva.

   La definizione della struttura menu viene salvata e compare la pagina Dettagli struttura menu.

Creazione e pubblicazione di un set di file della Guida

Si possono creare set di file della Guida in linea personalizzati per qualsiasi ruolo.

Per creare, riempire e pubblicare un set di file della Guida

1. Selezionare Gestione ruoli e protezione, Gestione ruoli, Set di file della Guida nella scheda Amministrazione.

   Compare la pagina Elenco set di file della Guida.

2. Fare clic su Crea Nuovo.

   Compare la pagina Crea nuovo set di file della Guida.

3. Inserire i dati nei seguenti campi:

   Nome set di file della Guida

   Il nome univoco del set di file della Guida.

   Tipo interfaccia

   Il tipo di interfaccia del set di file della Guida (ad esempio Analista, Dipendente o Cliente).

   Stato record

   Indica se il set di file della Guida è attivo o non attivo.

   Prefisso nome file

   Il prefisso da associare ai file generati per questo set di file della Guida. Non includere spazi nel nome.

   Nota: assegnare un prefisso che consenta di identificare i file che appartengono al set di file della Guida. Ad esempio, potrebbe essere utile utilizzare il prefisso ANAL per un set di file della Guida per gli analisti.

   Interna

   Questa opzione è impostata automaticamente su NO per i set di file della Guida definiti dall'utente. Il valore in questo gruppo non può essere modificato.

4. Fare clic su Salva.

   Viene visualizzata la scheda Contenuti.

5. Fare clic su Definire contenuto.

   Viene visualizzata la finestra Selected Help Update.

6. Selezionare il contenuto da includere nel set di file della Guida.

   Importante. alcuni argomenti sono obbligatori e sono inclusi automaticamente nel nuovo set di file della Guida. Ad esempio, gli argomenti per la pagina iniziale di CA SDM e altre premesse sono sempre inclusi. Inoltre, gli argomenti nidificati dipendono dai rispettivi argomenti di contenitore. Essi pertanto vengono inclusi automaticamente se si aggiungono i rispettivi argomenti nidificati. Ad esempio, se si utilizza l'argomento "Utilizzo del contatore", l'argomento di contenitore "Navigazione in CA SDM" verrà incluso quando si pubblica il set di file della Guida.

7. Fare clic su OK.

   La finestra Selected Help Update viene chiusa e i contenuti sono elencati nella scheda Contenuti.

8. Fare clic su Pubblica.

   Il set di file della Guida verrò generato raggruppando gli argomenti selezionati in un sistema di guida in linea che si può visualizzare in un browser Web.

9. Attendere il completamento del processo di pubblicazione, quindi selezionare Visualizza, Aggiorna nella barra dei menu.

   Il pulsante Visualizza guida in linea diventa attivo.

10. Fare clic su Visualizza guida in linea.

    Il set di file della Guida compare nel browser Web predefinito.

Cambio dei ruoli

Gli utenti a cui sono assegnati più ruoli possono passare da un ruolo a un altro senza dover uscire dal sistema e accedervi nuovamente. I ruoli sono assegnati agli utenti nel relativo Tipo di accesso o record contatto.

Nota: per informazioni, consultare Configurazione degli account utente (a pagina 319).

Per cambiare i ruoli

1. Selezionare il ruolo desiderato dall'elenco a discesa nell'angolo superiore destro della pagina principale di CA SDM.

2. Fare clic su Imposta ruolo.

   L'interfaccia Web e la funzionalità disponibile per l'utente connesso cambiano in base al ruolo corrente.

Capitolo 10: Definizione della struttura di supporto

Questa sezione contiene i seguenti argomenti:

Modelli (a pagina 385)
CA Workflow (a pagina 389)
Integrazione del flusso di lavoro di CA Process Automation (a pagina 392)
Codici condivisi (a pagina 398)
Codici stato (a pagina 401)
Tipi di attività (a pagina 406)
Aree Richiesta/Incidente/Problema (a pagina 408)
Categorie Ordine di cambiamento e Issue (a pagina 411)
Chiusura automatica dei ticket (a pagina 417)
Attività correlate ai ticket (a pagina 419)
Calcolo della priorità (a pagina 421)
Controlli di attributo dipendenti e transizioni di stato (a pagina 437)
Transizioni di stato per l'interfaccia self-service (a pagina 448)
Timer (a pagina 452)
Fusi orari (a pagina 453)
Modalità di configurazione della libreria allegati (a pagina 455)
Annunci (a pagina 465)
Configurazione delle query memorizzate (a pagina 467)
Numeri di sequenza (a pagina 468)
Uso del registro di audit (a pagina 469)
Integrazione con CA Network and Systems Management (a pagina 470)
Stampa di pagine Web CA SDM (a pagina 470)
Blocco dei record nell'interfaccia Web (a pagina 471)
Struttura di supporto (a pagina 471)
Abilitazione della Guida in linea di CAPA (a pagina 472)

Modelli

CA SDM supporta i modelli di service desk seguenti:

- Modello interno
- Modello esterno
- Modello combinato

Nota: per i dettagli sull'uso dell'interfaccia Web per implementare il modello selezionato, consultare la *Guida in linea*.

Modello interno

Un service desk interno supporta i dipendenti che lavorano per una società e che hanno domande o problemi relativamente ai prodotti forniti loro dalla società. In CA SDM, la richiesta rappresenta l'unità di base del supporto quando si utilizza un service desk interno, come descritto di seguito:

- Le richieste sono ticket che gestiscono le questioni o i problemi dei dipendenti. Il loro scopo è quello di fornire il supporto a un'infrastruttura di proprietà e amministrata dall'organizzazione di supporto.
- Gli ordini di cambiamento sono dei ticket che gestiscono i cambiamenti dell'infrastruttura del business supportata. I service desk interni spesso utilizzano le richieste come ticket primari, associandovi gli ordini di cambiamento nel caso in cui la richiesta ha come conseguenza una modifica all'infrastruttura.

Se si sta utilizzando un service desk interno, effettuare le seguenti operazioni:

- Esaminare il tipo di accesso dipendente utilizzando la funzione di amministrazione dell'interfaccia Web per verificare se soddisfa le proprie esigenze. Se la maggior parte dei contatti è rappresentata da dipendenti che utilizzano il service desk a scopo di supporto, potrebbe essere necessario impostare "dipendente" come tipo di accesso predefinito. In questo modo potrebbe non essere necessario dover impostare il tipo di accesso per ogni contatto di tipo dipendente supportato dal service desk.
- Esaminare il tipo di contatto dipendente utilizzando la funzione di amministrazione dell'interfaccia Web per verificare se soddisfa le proprie esigenze.
- Verificare che i contatti siano del tipo appropriato e impostati sul tipo di accesso corretto. Ad esempio, se dipendente è il tipo di accesso predefinito impostato, è necessario impostare i contatti analista sul tipo di accesso analista.

  Il tipo di contatto viene solitamente assegnato automaticamente in base al modo con cui viene creato il contatto ma, in alcuni casi, il tipo di contatto potrebbe non essere definito. Per i dipendenti che utilizzano il service desk a scopo di supporto, dovrebbe essere assegnato un tipo di contatto dipendente, mentre ai dipendenti che lavorano come analisti del service desk dovrebbe essere assegnato un tipo di contatto analista.

  È possibile lavorare con i contatti utilizzando la funzione di amministrazione dell'interfaccia Web.

Se si sta utilizzando un service desk interno per il supporto dei dipendenti, la struttura di supporto è costituita dalle richieste e dagli ordini di cambiamento creati dai dipendenti e dalle funzioni di supporto implicite relative a tali richieste e ordini di cambiamento. L'amministratore deve configurare la struttura di supporto.

Modello esterno

Un service desk esterno supporta i clienti che acquistano prodotti o servizi dalla società e che hanno domande o problemi relativamente a tali prodotti o servizi. In CA SDM, la questione rappresenta l'unità di base del supporto quando si utilizza un service desk esterno. Le questioni sono ticket destinati alla gestione delle domande o dei problemi del cliente e il loro scopo è quello di fornire il supporto per i prodotti e i servizi acquistati dal cliente.

Se si sta utilizzando un service desk esterno:

- Esaminare il tipo di accesso cliente utilizzando la funzione di amministrazione dell'interfaccia Web per verificare se soddisfa le proprie esigenze. Se la maggior parte dei contatti è rappresentata da clienti, potrebbe essere necessario impostare "cliente" come tipo di accesso predefinito.
- Esaminare il tipo di contatto cliente utilizzando la funzione di amministrazione dell'interfaccia Web per verificare se soddisfa le proprie esigenze.
- Verificare che i contatti siano del tipo appropriato e impostati sul tipo di accesso corretto. Ad esempio, se cliente è il tipo di accesso predefinito impostato, è necessario impostare i contatti analista sul tipo di accesso analista.

  Il tipo di contatto viene solitamente assegnato automaticamente in base al modo con cui viene creato il contatto ma, in alcuni casi, il tipo di contatto potrebbe non essere definito. Per i clienti che utilizzano il service desk a scopo di supporto, dovrebbe essere assegnato un tipo di contatto cliente, mentre agli analisti che utilizzano il service desk dovrebbe essere assegnato un tipo di contatto analista.

  È possibile lavorare con i contatti utilizzando la funzione di amministrazione dell'interfaccia Web.

Se si sta utilizzando un service desk esterno per il supporto dei clienti, la struttura di supporto è costituita essenzialmente dalle questioni create dai clienti e dalle funzioni di supporto implicite relative a tali questioni. L'amministratore, deve configurare la struttura di supporto utilizzando le informazioni contenute in questo capitolo. In ogni argomento viene indicato se le informazioni sono valide per il modello in uso.

Modello combinato

Alcune società hanno l'esigenza di utilizzare sia i modelli di service desk interni che quelli esterni. In questo caso, effettuare una delle seguenti operazioni:

- Separare i modelli di service desk interni ed esterni utilizzando installazioni diverse di Service Desk.
- Configurare CA SDM in modo che supporti entrambi i modelli.

  Questa configurazione è conveniente se gli analisti del service desk sono in grado di supportare sia i dipendenti sia i clienti e se la distinzione tra supporto interno ed esterno non è sempre netta. Ad esempio, è possibile che vi siano dei dipendenti che acquistano prodotti dalla propria società o clienti che hanno problemi e domande relativamente all'infrastruttura della società.

L'amministratore deve configurare la struttura di supporto per un service desk combinato (interno/esterno) che comprenda questioni, richieste e ordini di cambiamento, oltre alle relative funzioni di supporto. Se si decide di utilizzare un service desk combinato (interno/esterno), effettuare le seguenti operazioni prima di configurare una struttura:

- Esaminare i tipi di accesso cliente e dipendente utilizzando la funzione di amministrazione dell'interfaccia Web per verificare se soddisfano le proprie necessità. Se la maggior parte dei contatti è rappresentata da clienti, potrebbe essere necessario impostare "cliente" come tipo di accesso predefinito. Se la maggior parte dei contatti è rappresentata da dipendenti che utilizzano il service desk a scopo di supporto, potrebbe essere necessario impostare "dipendente" come tipo di accesso predefinito.
- Esaminare i tipi di contatto "cliente" e "dipendente" utilizzando la funzione di amministrazione dell'interfaccia Web per verificare se soddisfa le proprie necessità.
- Verificare che il tipo dei contatti sia corretto e che dispongano del tipo di accesso adeguato. Ad esempio, se cliente è impostato sul tipo di accesso predefinito impostato, è necessario impostare anche i contatti analista sul tipo di accesso analista e i contatti dipendente sul tipo di accesso dipendente.

  Il tipo di contatto viene solitamente assegnato automaticamente in base al modo con cui viene creato il contatto ma, in alcuni casi, il tipo di contatto potrebbe non essere definito.

  - Ai clienti che utilizzano il service desk a scopo di supporto, dovrebbe essere assegnato un tipo di contatto cliente.
  - Ai dipendenti che utilizzano il service desk a scopo di supporto dovrebbe essere assegnato un tipo di contatto dipendente.
  - Ai dipendenti che lavorano come analisti del service desk dovrebbe essere assegnato un tipo di contatto analista.

  È possibile lavorare con i contatti utilizzando la funzione di amministrazione dell'interfaccia Web.

Ulteriori informazioni:

Tipi contatto (a pagina 322)
Modalità di funzionamento dei tipi di accesso (a pagina 354)

CA Workflow

Una definizione di processo CA Workflow può essere associata con qualsiasi tipo di ticket (a pagina 61) CA SDM. La definizione di processo che viene applicata ai singoli ticket dipende dalla categoria del Cambiamento, della Issue o dall'area Richiesta/Incidente/Problema a cui è assegnato il ticket.

Se una definizione di processo CA Workflow è associata ad una categoria o ad un'area, quando un ticket viene assegnato alla categoria o all'area in questione, CA Workflow crea un'istanza del processo dalla definizione. L'avanzamento dell'istanza del processo viene visualizzato nella scheda Attività flusso di lavoro.

È possibile installare facoltativamente CA Workflow durante l'installazione di CA SDM o richiedere a CA SDM di utilizzare un'altra istanza di CA Workflow aggiornando le diverse opzioni disponibili Gestione opzioni, incluse le seguenti:

CAWF_USERNAME

Specifica l'utente CA EEM che ha accesso completo (per le risorse "IDE" e "Processo") a CA Workflow.

CAWF_PASSWORD

Specifica la password per l'opzione cawf_username.

CAWF_PM_LOCATION

Specifica la posizione: http://<server>:8090/pm/

CAWF_PM_URL

Specifica l'URL: http://<wf_hostname>:<wf_tomcat_port>/pm/services/pmService2

CAWF_WL_LOCATION

Specifica la posizione: http://<server>:8090/wl/

CAWF_WL_URL

Specifica l'URL: http://<server>:8090/wl/services/wlService

Queste opzioni specificano i diversi punti finali a CA Workflow. Nella maggior parte dei casi, aggiornare semplicemente il server e la porta in base alla posizione di CA Workflow.

Importante. se si modifica il server CA Workflow, vengono rese inattive le categorie, le aree o i ticket esistenti collegati per elaborare le definizioni e le istanze di processo sul vecchio server.

Flusso di lavoro in runtime

Quando un ticket viene salvato con una categoria o un'area collegata ad una definizione di processo CA Workflow, viene creata un'istanza della definizione. L'avanzamento dell'istanza viene visualizzato nella scheda Attività flusso di lavoro del ticket. Poiché CA Workflow potrebbe includere ramificazioni, vengono visualizzati solo gli elementi di lavoro completati e in sospeso.

Nella scheda Attività flusso di lavoro viene visualizzato ogni elemento di lavoro completato e in sospeso e lo stato dell'intero flusso di lavoro. Se si fa clic sul collegamento Nome attività, viene visualizzata l'applicazione Web Elenco di lavoro CA Workflow, utilizzata per completare singoli elementi di lavoro.

I dati della scheda Flusso di lavoro vengono caricati direttamente dal server CA Workflow. Se il server CA Workflow non è disponibile, nella scheda viene visualizzato un messaggio di errore.

Selezione di una definizione di processo CA Workflow

Una definizione di processo CA Workflow deve contenere un attributo di tipo string denominato *usd_persid* che collega a una categoria cambiamento o questione oppure a un'area di richiesta/incidente/problema. Questo attributo deve essere contrassegnato come un parametro di input. Quando CA SDM avvia l'istanza CA Workflow, imposta l'attributo usd_persid sull'identificatore univoco (persistent_id) del ticket. L'attributo usd_persid può essere utilizzato anche per effettuare le chiamate dei servizi Web da CA Workflow a CA SDM.

Importante le categorie cambiamento e questione possono utilizzare il sistema di flusso di lavoro interno (classico) di CA SDM o l'applicazione CA Workflow. I due metodi non possono essere combinati. Le aree richiesta/incidente/problema possono utilizzare solo l'applicazione CA Workflow. Il sistema del flusso di lavoro classico interno non è supportato per i ticket richiesta, incidente o problema.

Per selezionare una definizione di processo CA Workflow:

1. Selezionare una categoria cambiamento o questione. Per selezionare ad esempio una categoria cambiamento, selezionare Service Desk, Ordini di cambiamento, Categorie nella scheda Amministrazione.

   Viene visualizzata la pagina Elenco categorie cambiamento.

2. Fare clic sul simbolo della categoria cambiamento da modificare.

   Viene visualizzata la pagina Dettagli categoria cambiamento.

3. Fare clic sul pulsante Usa CA Workflow della scheda Flusso di lavoro.

   Nota: se si continua questa procedura e se si salva la categoria, tutti i flussi di lavoro di stile di CA SDM ad essa associati vengono automaticamente eliminati.

   Viene visualizzata una pagina di selezione che elenca le definizioni di processo CA Workflow disponibili.

4. Selezionare una definizione di processo CA Workflow.

   La categoria viene compilata con la selezione.

5. Fare clic su Salva.

   La categoria viene aggiornata con la definizione di processo selezionata.

6. (Facoltativo) Cambiare la definizione di processo CA Workflow collegata modificando la categoria e facendo clic sul collegamento ipertestuale della definizione CA Workflow.

   Viene visualizzata la pagina di selezione della definizione di processo.

   Nota: le definizioni di processo CA Workflow vengono visualizzate solo nella pagina di selezione, se la definizione contiene un attributo di tipo string denominato usd_persid. Quando la definizione viene avviata, questo attributo viene impostato sul valore del persistent_id del ticket. La definizione di processo CA Workflow può includere, facoltativamente, un parametro di input di tipo string denominato *label*. Se tale parametro è definito, CA SDM ne imposta il valore sul numero di ticket. Il numero di ticket viene visualizzato nell'elenco di lavoro CA Workflow e permette di fornire un contesto per l'elemento di lavoro.

Attività flusso di lavoro

Le attività flusso di lavoro identificano le attività completate nei ticket associati ad una specifica area o categoria. Come per le proprietà e altri aspetti della categoria o dell'area, le attività vengono automaticamente aggiunte ai ticket quando la categoria viene selezionata. La definizione delle attività del flusso di lavoro consente di effettuare quanto riportato di seguito:

- Specificare e descrivere il tipo di attività da completare.
- Assegnare un numero di sequenza a ogni attività.

- Specificare l'utente per il completamento dell'attività.
- Identificare l'avanzamento verso la risoluzione delle attività assegnando specifici stati validi per ogni attività.

Quando lo stato di un'attività cambia, possono verificarsi determinati comportamenti. I comportamenti consentono di definire le specifiche attività o i processi eseguiti quando l'attività del flusso di lavoro raggiunge uno stato specifico. Ad esempio, grazie alla definizione dei comportamenti è possibile inviare una notifica tramite posta elettronica a un responsabile quando l'attività di approvazione passa allo stato In sospeso.

Nota: per ulteriori informazioni su come creare le attività flusso di lavoro e definirne i comportamenti, consultare la *Guida in linea*.

Integrazione del flusso di lavoro di CA Process Automation

CA Process Automation è un prodotto CA autonomo con caratteristiche per l'automazione e il tracciamento di attività di amministrazione hardware e software in ambienti IT aziendali. CA Process Automation consente l'automazione di attività e gestisce le interazioni con l'utente, quali approvazioni e notifiche per la conformità e la precisione all'interno di ambienti di produzione.

Quando si integrano CA SDM e CA Process Automation, è possibile sfruttare i vantaggi delle funzionalità del flusso di lavoro di CA Process Automation da punti chiave in CA SDM. Per un'integrazione efficace di CA SDM e CA Process Automation è necessario conoscere entrambi i prodotti.

Ulteriori informazioni:

Componenti di CA Process Automation (a pagina 393)
Integrazione di CA Process Automation con CA SDM all'esecuzione (a pagina 393)
Modalità di creazione di una definizione di processo (a pagina 394)
Creazione di un modulo richiesta di avvio (a pagina 395)
Associazione di una definizione di processo di CA Process Automation (a pagina 397)

Componenti di CA Process Automation

CA Process Automation offre numerose funzionalità e strutture che facilitano una vasta gamma di attività nell'ambito della gestione dei processi CA Process Automation. Per l'integrazione con CA SDM, tuttavia, sono critici solo i seguenti componenti di CA Process Automation:

- **Definizione di processo—**Identifica una serie collettiva di attività, fasi e condizioni strutturate in un ordine specifico che vengono avviate e completate da vari individui o parti. Questo componente è l'elemento costitutivo centrale di tutto il contenuto di CA Process Automation.
- **Modulo richiesta di avvio—**Oggetto contenente informazioni descrittive per gli utenti finali. Il Modulo richiesta di avvio presenta una definizione di processo agli utenti nascondendone i dettagli tecnici.
- **Parole chiave—**Elenco di parole o frasi predefinite da associare a moduli richiesta di avvio.
- **Libreria di automazione—**Area in CA Process Automation in cui sono archiviate e visualizzate definizioni di processo e moduli richiesta di avvio.
- **Percorso della libreria o percorso di riferimento—**Struttura di cartelle che organizza e descrive definizioni di processo e moduli richiesta di avvio nella libreria di automazione.
- **Istanza di processo—**Entità attiva che esegue le regole definite nella definizione di processo. L'istanza di processo procede finché lo stato della definizione di processo è completo.
- **Messaggi di registro dell'istanza di processo—**Record configurabile che descrive la progressione delle attività dell'istanza di processo. Ai fini dell'integrazione di CA SDM con CA Process Automation sono utili le categorie dei messaggi di registro.

Nota: lo scopo delle definizioni dei componenti di CA Process Automation è limitato al loro utilizzo in CA SDM. Per informazioni su componenti e funzionalità di CA Process Automation, consultare la documentazione CA Process Automation.

Integrazione di CA Process Automation con CA SDM all'esecuzione

Quando si attiva l'integrazione, in CA SDM avviene quanto riportato di seguito:

- In una nuova richiesta, ordine di cambiamento o questione, viene iniziata un'istanza di processo di CA Process Automation in base all'area o categoria di ticket. Le informazioni riepilogative vengono immediatamente visualizzate nella scheda Attività flusso di lavoro.
- Quando cambia un'area richiesta, categoria cambiamento o categoria questione, termina un'istanza di processo di CA Process Automation associata e ne viene avviata un'altra.

- Quando un utente di CA SDM tenta di chiudere una richiesta, ordine di cambiamento o questione in cui l'istanza di processo di CA Process Automation non è ancora completa, l'utente non può chiudere il ticket. Per farlo, l'utente deve prima annullare il ticket. Lo stato Annulla termina l'istanza di processo di CA Process Automation prima che il ticket venga chiuso.
- Quando un utente desidera conoscere lo stato dell'istanza di processo senza uscire dal ticket, può farlo facendo clic sulla scheda Attività flusso di lavoro del ticket. Nella scheda Attività flusso di lavoro sono visualizzati la data di inizio, la data di fine e lo stato corrente dell'istanza di processo e un itinerario di controllo corrente dei messaggi che indica il percorso dell'istanza di processo.
- Quando un utente desidera vedere il percorso corrente dell'istanza di processo relativa all'intero processo, seleziona il pulsante Visualizza processo nella scheda Attività flusso di lavoro. Il pulsante Visualizza processo avvia un'istantanea grafica dell'intera istanza di processo e mostra il percorso corrente.
- Quando un utente desidera vedere moduli di richiesta di interazione di CA Process Automation in attesa dell'azione da parte dell'utente, l'utente può selezionare qualsiasi voce nella scheda Attività flusso di lavoro. La scheda Attività flusso di lavoro contiene un itinerario di controllo dei messaggi di istanza di processo che compaiono nell'elenco delle attività di CA Process Automation.

Nota: quando un utente seleziona il pulsante Visualizza processo di CA SDM o messaggi di istanza di processo di CA Process Automation, vengono richiesti un nome utente e una password CA Process Automation per un'unica sessione del browser. Dopo il prompt iniziale, non ne vengono visualizzati altri finché il browser di CA SDM non viene chiuso.

Modalità di creazione di una definizione di processo

Quando si crea la definizione di processo, si compila CA Process Automation con il contenuto visualizzato in CA SDM. Per creare, testare e archiviare la definizione di processo, si utilizza lo strumento di progettazione grafica dei processi di CA Process Automation. Da CA SDM è anche possibile creare macro per iniziare processi CA Process Automation.

Nota: per informazioni sulla creazione di marco CA Process Automation, consultare la *Guida in linea*.

Per creare una definizione di processo in CA Process Automation, procedere come segue:

1. Accedere al client CA Process Automation come utente amministrativo.

2. Per creare, testare e archiviare la definizione di processo, utilizzare lo strumento di progettazione grafica dei processi di CA Process Automation. Quando si lavora alla definizione di processo, attenersi alle istruzioni riportate nella documentazione utente di CA Process Automation.

   Nota: se non si archivia la definizione di processo prima di tentare di usarla, il flusso di lavoro non può funzionare correttamente in CA SDM.

   In CA SDM sono disponibili i seguenti elementi di definizione di processo:

   Nome elaborazione

   Compare nelle pagine Dettagli area richiesta, Dettagli categoria cambiamento e Dettagli questione. Il nome del processo viene inoltre visualizzato nella scheda Attività flusso di lavoro di un ticket. Il nome del processo descrive la definizione di processo agli analisti di CA SDM e ad altri utenti che gestiscono i ticket.

   Percorso di riferimento del processo

   Compare nelle pagine Dettagli area richiesta, Dettagli categoria cambiamento e Dettagli questione. Il percorso di riferimento del processo compare inoltre nella scheda Attività flusso di lavoro del ticket. Il percorso di riferimento del processo può essere utile per descrivere lo scopo del processo agli utenti finali. Ad esempio, "/Processi/Approvazione" non è un percorso utile, mentre un percorso di riferimento come "/Cancelleria/Approvazioni/Superiori-a-200-Euro" descrive il flusso di lavoro per la gestione di ordini superiori a 200€.

   Messaggi del registro di processo

   Vengono visualizzati nella scheda Attività flusso di lavoro del ticket CA SDM. Per impostazione predefinita, un record di attività viene archiviato con l'istanza di processo. I messaggi del registro di processo hanno la categoria Processo. Uno strumento di progettazione processi può creare messaggi personalizzati da visualizzare nella scheda Attività flusso di lavoro di un ticket CA SDM.

   Nota: per informazioni sulla configurazione dell'opzione caextwf_log_categories per gestire messaggi di registro, consultare la *Guida all'implementazione*.

Creazione di un modulo richiesta di avvio

Quando si crea un modulo richiesta di avvio, lo si associa alla definizione di processo e lo si archivia. Nelle proprietà del modulo richiesta di avvio si includono le parole chiave appropriate. Se nelle proprietà del modulo richiesta di avvio mancano le parole chiave appropriate, il modulo e la definizione di processo ad esso associata non compaiono in CA SDM.

Per creare un modulo richiesta di avvio

1. Accedere al client CA Process Automation come utente amministrativo.
2. Aprire la libreria di CA Process Automation e individuare il percorso del modulo richiesta di avvio.

   Il modulo richiesta di avvio viene visualizzato nel riquadro di destra della libreria di CA Process Automation.
3. Selezionare Modulo richiesta di avvio dal'elenco.

   Viene visualizzato un menu di scelta rapida.
4. Selezionare Proprietà.

   Viene visualizzata la pagina delle proprietà dell'oggetto della libreria.
5. (Facoltativo) Fare clic sulla scheda Generale e modificare la descrizione del modulo richiesta di avvio. Aggiungere una descrizione che identifichi l'utilizzo appropriato del modulo richiesta di avvio e la definizione di processo associata all'amministratore di CA SDM.
6. Fare clic sulla scheda Parole chiave.

   La scheda Parole chiave è attiva.
7. Fare clic sull'icona ab+.

   Nell'elenco vuoto viene aggiunta una riga.
8. Fare clic sulla riga.

   Un cursore lampeggiante evidenzia la riga e indica che la riga è pronta per la digitazione.
9. Immettere uno dei seguenti valori per associare una parola chiave all'area o alla categoria del ticket appropriata. Ad esempio, per rendere un modulo richiesta di avvio disponibile per un'area richiesta di CA SDM, immettere la parola chiave pcat.

Ticket	Utilizzare parola chiave
area richiesta	pcat
categoria cambiamento	chgcat
categoria questione	isscat

10. Aggiungere una riga all'elenco per ogni parola chiave applicabile. Ad esempio, affinché il Modulo richiesta di avvio compaia sia nelle aree richiesta che nelle categorie cambiamento, aggiungere una riga per la parola chiave chgcat e un'altra riga per la parola chiave pcat.
11. Fare clic su OK.

    La parole chiave e la descrizione vengono salvate e viene chiusa la finestra di dialogo delle proprietà dell'oggetto delle libreria.

12. Archiviare il modulo richiesta di avvio.

    Nota: se non viene archiviato, il modulo richiesta di avvio non viene visualizzato in CA SDM.

    Le informazioni del modulo richiesta di avvio di CA Process Automation vengono visualizzate nell'Elenco moduli richiesta di avvio di CA SDM. L'amministratore di CA SDM può associare il modulo richiesta di avvio di CA SDM con la definizione di processo in una pagina Dettagli area richiesta, Dettagli categoria cambiamento o Dettagli categoria questione.

    In CA SDM vengono visualizzati i seguenti elementi del modulo richiesta di avvio:

    Nome del modulo richiesta di avvio

    Compare nelle pagine Elenco aree richiesta, Elenco categorie cambiamento e Elenco categorie questione.

    Percorso di riferimento del modulo richiesta di avvio

    Compare nelle pagine Elenco aree richiesta, Elenco categorie cambiamento e Elenco categorie questione.

    Descrizione del modulo richiesta di avvio

    Compare nelle pagine Elenco aree richiesta, Elenco categorie cambiamento e Elenco categorie questione. Il testo in questo campo descrive come il modulo richiesta di avvio sia appropriato per la selezione in una determinata area richiesta, categoria cambiamento o categoria questione.

Associazione di una definizione di processo di CA Process Automation

Quando si associa una definizione di processo di CA Process Automation a un'area o categoria di ticket di CA SDM, si crea una connessione statica tra un'area o categoria di ticket di CA SDM e una definizione di processo di CA Process Automation.

Quando un utente di CA SDM crea o modifica un ticket e seleziona una categoria di ticket, la definizione di processo di CA Process Automation associata avvia un'istanza di processo. Le informazioni pertinenti sull'istanza di processo vengono visualizzate nella scheda Attività flusso di lavoro del ticket.

Per associare una definizione di processo di CA Process Automation

1. Nella scheda Amministrazione, selezionare Service Desk.
2. Accedere alle Aree o Categorie ticket.

   Viene visualizzato l'Elenco aree o categorie.

3. Creare o modificare un'area o categoria di ticket.

   Viene visualizzata la pagina Aggiorna.

4. Fare clic sulla scheda Flusso di lavoro.

   Se in Gestione opzioni di CA SDM sono installate le Opzioni di CA Process Automation, nella scheda Flusso di lavoro è disponibile il pulsante Utilizzare CA IT PAM.

5. Fare clic sul pulsante Utilizzare CA IT PAM.

   Viene visualizzato l'elenco Moduli richiesta di avvio di CA IT PAM. Ogni riga dell'elenco corrisponde a un modulo di richiesta di avvio di CA Process Automation.

   Nota: è possibile utilizzare CA Process Automation, CA Workflow o il flusso di lavoro interno di CA SDM per gestire varie aree o categorie di ticket. Tuttavia, una categoria può utilizzare un solo strumento di flusso di lavoro alla volta.

6. Fare clic sul valore nella colonna Nome per selezionare la definizione di processo associata al modulo richiesta di avvio.

   L'elenco Moduli richiesta di avvio di CA IT PAM viene chiuso. Il nome e il percorso di riferimento della definizione di processo vengono visualizzati nella scheda Flusso di lavoro.

7. Fare clic su Salva.

   Il sistema salva le impostazioni di processo. Al successivo ticket creato da un utente nell'area o categoria di ticket specificata verrà associato automaticamente il flusso di lavoro e verrà creata un'istanza di processo. Nella scheda Attività flusso di lavoro viene mostrato un riepilogo delle informazioni dell'istanza di processo. Un utente può inoltre accedere a ulteriori informazioni sull'istanza di processo facendo clic su Visualizza processo nella scheda Attività flusso di lavoro.

Codici condivisi

In CA SDM, più tipi di ticket condividono codici specifici, ad esempio i codici di priorità, gravità, impatto e urgenza. Le Richieste e gli Ordini di cambiamento condividono alcuni codici, mentre altri vengono condivisi da tutti i tipi di ticket.

Considerare le seguenti informazioni sui codici condivisi:

- Per impostazione predefinita, vengono utilizzati valori numerici per classificare i codici.
- È possibile personalizzare i codici.
- Non è possibile aggiungere o eliminare i codici condivisi.
- È possibile utilizzare codici di impatto, priorità, gravità e urgenza.

In base al modello di service desk utilizzato, impostare i codici seguenti:

Codici condivisi	Descrizione
Priorità	Deve essere impostato per tutti i modelli di service desk.
Gravità	Deve essere impostato per i modelli di service desk interni e combinati.
Impact	Deve essere impostato per i modelli di service desk interni e combinati.
Urgenza	Deve essere impostato per i modelli di service desk interni e combinati.

Nota: per informazioni dettagliate su come personalizzare i codici utilizzando la funzione di amministrazione dell'interfaccia Web, consultare la *Guida in linea*.

Ulteriori informazioni:

Codici di priorità (a pagina 399)
Codici di gravità (a pagina 400)
Codici di impatto (a pagina 400)
Codici di urgenza (a pagina 400)

Codici di priorità

I codici di priorità indicano l'ordine di classificazione in base al quale il service desk dovrebbe rispondere ai ticket, ovvero il livello di attenzione di un ticket. Ai codici di priorità viene fatto riferimento nelle richieste, negli ordini di cambiamento e nelle questioni, quindi sono validi per tutti i modelli di service desk.

È possibile utilizzare le priorità per riassegnare manualmente o automaticamente i ticket monitorando gli eventi. In molte installazioni di service desk, i codici di priorità vengono utilizzati nel segnapunti per fornire agli analisti lo stato delle richieste e degli ordini di cambiamento in tempo reale.

È possibile assegnare un tipo di servizio a un codice di priorità, che viene quindi assegnato automaticamente ai ticket quando il codice di priorità viene specificato. Ciò consente di associare un livello di servizio specifico a un ticket in base alla priorità assegnata. Il tipo di servizio definito dal sistema, ovvero la risoluzione in quattro ore, viene ad esempio automaticamente associato alla priorità 1. Ai ticket, cui viene assegnata la priorità 1 viene automaticamente assegnato questo tipo di servizio, inclusi tutti i relativi eventi associati al tipo di servizio per la risoluzione in quattro ore.

Ulteriori informazioni:

SLA (Service Level Agreement) (a pagina 253)

Codici di gravità

I codici di gravità identificano la misura del danno all'attrezzatura interessata da una richiesta. Ai codici di gravità viene fatto riferimento solo nelle richieste, quindi sono validi solo per i modelli di service desk interni e combinati.

Nota: la gravità viene spesso utilizzata come sinonimo di priorità. Alcuni siti utilizzano solo la priorità e ignorano completamente la gravità. Se si desidera fare una distinzione tra la gravità di un problema a livello tecnico (gravità) e la rapidità con la quale si desidera che il problema venga gestito (priorità), è possibile utilizzarli entrambi.

I valori del codice d'impatto vengono utilizzati per il calcolo della priorità dell'Incidente.

Codici di impatto

I codici di impatto misurano l'importanza di un ticket relativamente al funzionamento del sistema. Ad esempio, se un ordine di cambiamento influenza il funzionamento dell'intero sistema, gli verrà assegnato un livello di impatto alto. Ai codici di impatto viene fatto riferimento solo nelle richieste e negli ordini di cambiamento, quindi sono validi solo per i modelli di service desk interni e combinati.

Nota: i codici di impatto e di urgenza (a pagina 400) sono simili, ma il loro scopo è differente.

Codici di urgenza

I codici di urgenza misurano l'importanza della richiesta per gli utenti del sistema, ovvero indicano l'importanza della richiesta relativamente all'intero ambiente di produzione. Se ad esempio una richiesta può compromettere la missione dell'azienda, il codice di urgenza può corrispondere al valore 5-Immediato. Ai codici di urgenza viene fatto riferimento solo nelle richieste, quindi sono validi solo per i modelli di service desk interni e combinati.

Gli scopi dei codici di urgenza e di impatto sono differenti ma spesso vengono confusi poiché coincidono. Una richiesta per segnalare un incendio in un importante centro dati può ad esempio presentare un impatto 3-Gruppo singolo e un'urgenza 5-Immediato. Questi codici si applicano in quanto l'impatto dell'incendio riguarda più gruppi ma non necessariamente l'intera organizzazione. Poiché il centro dati è fondamentale per le operazioni, l'urgenza richiede un intervento immediato.

Codici stato

I codici di stato vengono utilizzati per tenere traccia dello stato di un elemento. Codici di stato separati consentono di tenere traccia di Richieste, Ordini di cambiamento, Issue e attività del flusso di lavoro. In ogni caso, sono disponibili codici di stato predefiniti che è possibile utilizzare in base alle specifiche esigenze. In alternativa, è possibile modificare i codici di stato predefiniti o definire nuovi codici di stato specifici per il proprio sito. In base al modello di service desk utilizzato, impostare i codici seguenti:

Codici stato	Descrizione
Richiesta	Deve essere impostato per i modelli di service desk interni e combinati.
Ordine di cambiamento	Deve essere impostato per i modelli di service desk interni e combinati.
Issue	Deve essere impostato per i modelli di service desk esterni e combinati.
Attività	Deve essere impostato per tutti i modelli di service desk.

I codici di stato consentono agli analisti di ordinare e selezionare le informazioni in base allo stato, in modo che possano tenerne una traccia accurata. L'accuratezza con cui vengono definiti i codici di stato determina la precisione con la quale gli analisti possono descrivere lo stato corrente di un elemento.

I codici di stato possono essere contrassegnati come attivi o non attivi. Quando si contrassegna un codice di stato come non attivo, non è più disponibile agli analisti ma rimane comunque disponibile per un utilizzo futuro, in quanto non viene eliminato dal database. Se in seguito si decide di utilizzare il codice di stato, è sufficiente contrassegnarlo come attivo.

Nota: le stesse definizioni di area sono disponibili per ticket Richiesta, Incidente e Problema. Nella scheda Amministrazione queste aree sono definite aree Richiesta/Incidente/Problema. Per ragioni di sintesi, qui si fa riferimento semplicemente ad aree Richiesta.

Codici stato richiesta

Nella tabella seguente vengono illustrati i codici stato predefiniti per i ticket richiesta.

Codice stato richiesta	Descrizione
Rilevato	La ricezione di una richiesta è stata riconosciuta.

Codice stato richiesta	Descrizione
Chiuso	Una richiesta è stata completamente risolta.
Chiuso—Non risolto	Una richiesta è stata chiusa ma deve ancora essere risolta.
Correzione in corso	Per una richiesta è in corso una correzione.
In attesa	Gli eventi tipo di servizio per la richiesta sono in attesa.
Open (Aperto)	È stata definita una richiesta che viene utilizzata per monitorarne e gestirne il completamento.
Problema chiuso	Un problema è stato completamente chiuso.
Problema corretto	Un problema è stato corretto, ma non chiuso.
Problema aperto	Una richiesta è stata identificata come un problema.
Researching	Una richiesta è aperta è vi sono ricerche e analisi aggiuntive in sospeso.
Operazione in corso	È in corso un'operazione per correggere una richiesta.

Se il proprio sito utilizza un'altra terminologia per identificare lo stato di una richiesta, sarebbe opportuno definire i codici di stato in base alle specifiche esigenze e ignorare i codici di stato predefiniti oppure modificare le definizioni nel modo appropriato. Ad esempio, è possibile definire codici stato richiesta aggiuntivi quali:

Codice stato richiesta	Descrizione
Duplicato	Richieste che sono state aperte ma che potrebbero essere duplicati di richieste esistenti di altri utenti.
Emergency	Richieste critiche che devono essere inoltrate immediatamente.
Rapporto	Richieste risolte e chiuse ma che devono essere segnalate al livello di gestione.
Test	Richieste risolte ma di cui è necessario eseguire il test per una settimana per poter essere chiuse.

Codici stato ordine di cambiamento

Nella tabella seguente vengono illustrati i codici stato predefiniti per i ticket ordine di cambiamento.

Codice stato ordine di cambiamento	Descrizione
Approvazione in corso	Un ordine di cambiamento è aperto e l'approvazione è in sospeso.
Approvato	Un ordine di cambiamento è stato approvato.
Annullato	Un ordine di cambiamento è stato annullato.
Chiuso	Un ordine di cambiamento è stato completato.
In attesa	Gli eventi tipo di servizio per l'ordine di cambiamento sono in attesa.
Implementazione in corso	È in corso l'implementazione di un ordine di cambiamento.
Open (Aperto)	In un ordine di cambiamento è stato definito un ordine di servizio e l'ordine di cambiamento viene utilizzato per monitorarne e gestirne il completamento.
Rifiutato	Un ordine di cambiamento è stato rifiutato.
Risolto	Un ordine di cambiamento è stato risolto.
RFC	Una richiesta di cambiamento è stata inviata.
Sospesa	Arresta le attività del flusso di lavoro in un ordine di cambiamento.
Verifica in corso	È in corso la verifica di un ordine di cambiamento.
Ritirato	L'ordine di cambiamento implementato è stato ritirato.
Implementato	Il cambiamento è stato implementato.

Se il proprio sito utilizza un'altra terminologia per identificare lo stato di un ordine di cambiamento. sarebbe opportuno definire i codici di stato in base alle specifiche esigenze e ignorare i codici di stato predefiniti oppure modificare le definizioni nel modo appropriato. Ad esempio, è possibile definire codici stato ordine di cambiamento aggiuntivi, ad esempio quelli riportati nella tabella seguente:

Codice stato richiesta personalizzata	Descrizione
Duplicato	Gli ordini di cambiamento che sono stati aperti ma che potrebbero essere duplicati di ordini di cambiamento esistenti di altri utenti.
Emergency	Ordini di cambiamento critici che devono essere inoltrati immediatamente.
Rapporto	Ordini di cambiamento risolti e chiusi ma di cui deve essere creato un rapporto a livello di gestione.

Codici di chiusura

I codici di chiusura consentono di definire il risultato finale degli ordini di cambiamento, ad esempio se sono riusciti o meno. Impostare i codici di chiusura manualmente o all'interno dell'aggiornamento degli stati di un ordine di cambiamento quando lo stato è chiuso, completati o risolto.

Nota: per ulteriori informazioni sulla creazione o la definizione dei codici di chiusura e sui dettagli delle opzioni *require_closure_code* e *force_closure_code*, vedere la *Guida in linea*.

Codici stato questione

Nella tabella seguente vengono illustrati i codici stato predefiniti per i ticket questione.

Codice stato questione	Descrizione
Approvazione in In corso	Una questione è aperta e l'approvazione è in corso.
Annullato	Una questione è stata annullata.
Chiuso	Una questione è stata completata.
In attesa	Gli eventi tipo di servizio per la questione sono in attesa.
Implementazione in corso	È in corso l'implementazione di una questione.
Open (Aperto)	Una questione è stata definita e aperta, in modo che sia possibile monitorarla e gestirla fino alla risoluzione.
Sospesa	Arresta le attività del flusso di lavoro in una questione.
Transazione in corso	È in corso una transazione con un cliente riguardante la questione.
Verifica in In corso	È in corso la verifica di una questione.

Se il proprio sito utilizza un'altra terminologia per identificare lo stato di una questione, sarebbe opportuno definire i codici di stato in base alle specifiche esigenze e ignorare i codici di stato predefiniti oppure modificare le definizioni nel modo appropriato. È ad esempio possibile definire codici stato questione aggiuntivi quali:

Codice stato questione personalizzata	Descrizione
Duplicato	Questioni che sono state aperte ma che potrebbero essere duplicati di questioni esistenti di altri utenti.

Codice stato questione personalizzata	Descrizione
Emergency	Questioni critiche che devono essere inoltrate immediatamente.
Rapporto	Questioni risolte e chiuse ma di cui deve essere creato un rapporto a livello di gestione.

Codici stato attività

I codici stato attività descrivono i possibili stati di un'attività del flusso di lavoro. Ogni attività in un flusso di lavoro relativo a una questione oppure a un ordine di cambiamento ha il proprio stato, separato dallo stato del ticket. Le attività del flusso di lavoro consentono agli analisti di tenere traccia del tempo impiegato per il completamento di singole attività in un ticket.

Nella tabella seguente vengono illustrati i codici stato predefiniti per le attività del flusso di lavoro.

Codice stato attività	Descrizione
Approva	L'attività è approvata.
Annullato	L'attività è annullata e non sono possibili ulteriori aggiornamenti.
Completa	L'attività è completata.
In sospeso	L'attività è avviata.
Rifiuta	L'attività è rifiutata.
Riapri	L'attività è stata-riaperta.
Riapri–Attendere	Un'attività precedente è stata riaperta.
Ignora	Ignora l'attività.
Attendere	L'attività non è stata avviata.

Se il proprio sito utilizza un'altra terminologia per identificare lo stato di un'attività del flusso di lavoro, sarebbe opportuno definire i codici di stato in base alle specifiche esigenze e ignorare i codici di stato predefiniti oppure modificare le definizioni nel modo appropriato.

Per ogni codice stato attività è possibile assegnare un tipo di comportamento che si verifica quando l'attività raggiunge uno stato specifico, attività che fornisce molte più informazioni sullo stato di completamento dell'attività. Inoltre, è possibile utilizzare la funzione di accumulo per tenere traccia del tempo e dei costi richiesti per il completamento del ticket.

Tipi di attività

I tipi di attività consentono di determinare il comportamento di specifiche attività del flusso di lavoro e i codici stato attività. Per la definizione delle caratteristiche di ciascun tipo di attività, è possibile identificare i codici stato attività che possono essere utilizzati.

Poiché gli ordini di cambiamento e le questioni utilizzano entrambi le attività del flusso di lavoro, impostare i tipi di attività per tutti i modelli di service desk. I codici stato attività identificano i comportamenti associati a ogni attività. Ad esempio, è possibile impostare il tipo di attività Approvazione per consentire Approva, Rifiuta, In sospeso e Attendere come stati disponibili. Quando il tipo di attività Approva passa allo stato In sospeso, è possibile inviare una notifica a uno specifico responsabile, analista e così via.

I tipi di attività possono essere contrassegnati come attivi o non attivi. Quando si contrassegna un tipo di attività come non attivo, non è più disponibile agli analisti ma rimane comunque disponibile per un utilizzo futuro, in quanto non viene eliminato dal database. Se in seguito si decide di utilizzare il tipo di attività, contrassegnarlo di nuovo come attivo.

Nota: nella pagina Elenco tipo attività della funzione di amministrazione dell'interfaccia Web è possibile visualizzare tutti i tipi di attività predefiniti.

Esempio: Codici stato attività

La seguente tabella contiene alcuni codici stato di esempio:

Codice stato attività	Descrizione
Approvazione	Approvazione o rifiuto del ticket
Fine attività gruppo	Fine delle attività del gruppo
Avvio attività gruppo	Avvio delle attività del gruppo
Avvio approvaz	Approvazione per l'avvio del ticket

In questo esempio i tipi di attività Avvio attività gruppo e Fine attività gruppo definiscono un gruppo di attività in una categoria questione o modifica da completare. Le attività nel gruppo possono essere eseguite in qualsiasi ordine. Quando Avvio attività gruppo si trova in stato In sospeso (avviato), questo stato viene applicato anche a tutte le attività del gruppo.

Nota: per ulteriori informazioni sull'uso dei tipi di attività, consultare la *Guida in linea*.

Il tracciato dell'Incidente consente agli analisti di tenere traccia di un Incidente selezionando uno o più flag per l'Incidente. Le informazioni specificate dagli analisti offrono all'organizzazione metriche relative agli IncidentI utili ai fini del reporting. Ad esempio, gli analisti possono indicare che un Incidente è stato assegnato in modo non corretto. Quando in un report compare una grande percentuale di ticket assegnati in modo errato, l'organizzazione sa che è necessario modificare le assegnazioni.

Ad esempio, gli analisti possono specificare informazioni per aiutare l'organizzazione a:

- Migliorare i tempi di risposta e chiusura SLA a livelli inferiori all'interno dell'organizzazione di supporto.
- Identificare ticket assegnati in modo non corretto.
- Indicare che per risolvere il ticket è stato utilizzato uno strumento di controllo remoto.

Per tracciare gli Incidenti è necessario installare l'opzione efficiency_tracking di Gestione opzioni, che consente agli analisti di utilizzare le opzioni della scheda Tracciato dell'efficienza delle pagine dei dettagli degli Incidenti.

Nota: per ulteriori informazioni sul tracciato degli Incidenti, consultare la *Guida in linea*.

Installazione del tracciamento degli incidenti

È possibile installare un'opzione che consente agli analisti di tenere traccia di un incidente impostando flag specifici. Le informazioni specificate dagli analisti offrono all'organizzazione metriche relative agli incidenti utili ai fini del reporting. Dopo aver installato l'opzione, i flag di tracciamento vengono visualizzati nella scheda Tracciato dell'efficienza delle pagine dei dettagli degli incidenti.

Per installare il tracciamento degli incidenti

1. Nella scheda Amministrazione, accedere a Gestione opzioni, quindi a Gestione richiesta.

   Viene visualizzato l'Elenco opzioni.

2. Fare clic su efficiency_tracking.

   Viene visualizzata la pagina Dettagli opzioni efficiency_tracking con l'insieme di valori predefiniti.

3. Fare clic su Modifica.

   Viene visualizzata la pagina Aggiorna opzioni efficiency_tracking con l'insieme di valori predefiniti, in cui è possibile modificare la descrizione.

4. Fare clic su Installa.

   Viene visualizzata la pagina Dettagli opzioni efficiency_tracking.

5. Fare clic su Chiudi finestra.

   Il tracciamento degli incidenti è installato, tuttavia la scheda Tracciato dell'efficienza non viene visualizzata nelle pagine dei dettagli degli incidenti.

6. Riavviare CA SDM.

   La scheda Tracciato dell'efficienza viene visualizzata nelle pagine dei dettagli degli incidenti.

Aree Richiesta/Incidente/Problema

Le aree Richiesta definiscono i raggruppamenti logici in base ai quali è possibile organizzare i ticket di Richiesta, Incidente e Problema. I ticket riguardanti un'applicazione possono ad esempio essere assegnati all'area Applicazioni predefinita. Quando un analista assegna un ticket ad un'area richiesta, tutte le informazioni associate all'area richiesta vengono immesse automaticamente nel ticket. Ad esempio, se si indica un tipo di servizio, questo viene associato al ticket e a tutti gli eventi tipo di servizio associati.

Nota: le stesse definizioni di area sono disponibili per ticket Richiesta, Incidente e Problema. Nella scheda Amministrazione dell'interfaccia Web di CA SDM queste aree vengono definite aree Richiesta/Incidente/Problema. Per ragioni di sintesi, qui si fa riferimento semplicemente ad aree Richiesta.

È possibile impostare lo stato di qualsiasi area Richiesta su Attivo o Non attivo. Quando una Richiesta viene resa inattiva, non è più disponibile per l'analista, ma non viene eliminata dal database. Se in seguito si decide di utilizzare l'area Richiesta, è sufficiente reimpostare lo stato su Attivo.

È possibile utilizzare le aree Richiesta per effettuare le operazioni seguenti:

- Specificare i valori predefiniti per i campi dei gruppi e degli assegnatari sui ticket.
- Associare automaticamente un livello di servizio ai ticket assegnando un tipo di servizio predefinito all'area Richiesta.
- Associare un'indagine a un'area Richiesta.
- Definire aree Richiesta personalizzate per selezionare e creare report sui ticket in base all'area. Esaminare la tendenza della Richiesta e analizzare le cause del Problema Concentrare l'attenzione verso aree Richiesta specifiche consente di ottenere un'analisi più significativa e dettagliata.

In CA SDM sono installate le seguenti aree Richiesta predefinite:

- Applicazioni
- Posta elettronica
- Hardware

- Reti
- Stampante
- Software

  L'area Software è suddivisa in diverse aree richiesta.

Nota: per informazioni sulla definizione e sulla modifica delle aree Richiesta, consultare la *Guida in linea*.

Ulteriori informazioni:

Proprietà area richiesta/incidente/problema (a pagina 409)
Definizione di aree richiesta/incidente/problema per l'interfaccia self-service (a pagina 411)

Proprietà area richiesta/incidente/problema

È possibile utilizzare le proprietà per aggiungere attributi o qualità personalizzate a un'area richiesta specifica. Se sono state aggiunte delle proprietà ad un'area di richiesta, quando un analista assegna un ticket a quell'area, le proprietà associate compaiono automaticamente nella scheda Proprietà del ticket. Ad esempio, si possono aggiungere proprietà all'area richiesta predefinita della posta elettronica per specificare la dimensione del server di posta elettronica o della casella di posta.

Quando si definiscono le proprietà è possibile specificare se un valore è richiesto o facoltativo. Per le proprietà con un valore obbligatorio (a pagina 410), gli utenti devono immettere un valore o accettare quello predefinito prima di poter salvare il ticket.

L'opzione keep_tasks determina ciò che accade quando si assegna un ticket esistente ad un'altra area richiesta:

- Se l'opzione keep_tasks non è installata, le proprietà esistenti (e le attività flusso di lavoro) vengono rimosse dal ticket e vengono aggiunte tutte le proprietà o le attività associate alla nuova area richiesta.
- Se l'opzione keep_tasks è installata, le attività e le proprietà esistenti vengono mantenute nel ticket e vengono aggiunte tutte le proprietà o le attività associate alla nuova area richiesta.

Nota: per istruzioni dettagliate su come aggiungere le proprietà a un'area richiesta e definire le regole di validazione delle proprietà, consultare la *Guida in linea*.

Regole di validazione proprietà

È possibile definire regole di validazione per stabilire una serie di valori predefiniti ai quali possono accedere gli utenti. Ad esempio, se si definisce una proprietà chiamata Sistema operativo, è possibile stabilire una regola di validazione sotto forma di elenco a discesa con le opzioni Windows, UNIX e Linux.

Le proprietà definite senza regole di validazione sono visualizzate come caselle di testo libero, in cui è possibile immettere qualsiasi stringa di testo. Le regole di validazione semplificano il processo di reporting sui valori per aree e categorie e lo rendono meno esposto a errori.

Nota: le regole di validazione delle proprietà sono riutilizzabili. Non sono specifiche di una determinata proprietà. È possibile applicare qualsiasi regola di validazione esistente alle proprietà definite per categorie cambiamento e questione o aree richiesta/incidente/problema.

A seconda del tipo di regola di validazione configurata per una proprietà, quando l'utente assegna un ticket alla categoria o all'area a cui è associata la proprietà, viene visualizzato uno dei controlli seguenti sulla scheda Proprietà del ticket:

- Casella di modifica del testo—Non è stata definita alcuna regola di validazione e non è possibile specificare alcun valore predefinito. Gli utenti devono immettere valori che seguano gli esempio forniti.
- Casella di controllo—Casella di controllo con due stati visualizzata nella scheda Proprietà. Per impostazione predefinita, la casella di controllo non contiene un segno di spunta. L'utente può accettare il valore predefinito o selezionare la casella di controllo. Le caselle che contengono un segno di spunta sono visualizzate sulla pagina Dettagli del ticket, con la dicitura Sì nella colonna del valore. Per le caselle deselezionate nella colonna del valore viene visualizzato No.
- Elenco a discesa—Elenco a discesa contenente un set predefinito di opzioni visualizzato nella scheda Proprietà. Se è stato definito un valore predefinito, viene selezionato quando l'elenco di elenco viene visualizzato la prima volta. L'opzione selezionata dall'utente compare nella colonna del valore nella pagina Dettagli del ticket.

Definizione di aree richiesta/incidente/problema per l'interfaccia self-service

È possibile utilizzare l'opzione Includi in self-service per definire quali aree richiesta/incidente/problema includere nei ticket per il self-service. È anche possibile definire simboli di self-service diversi rispetto a quelli visti dall'analista. Al salvataggio del ticket, il simbolo di self-service compare nel campo Area richiesta/incidente/problema. Se il ticket viene visualizzato nell'interfaccia dell'analista, per l'area viene visualizzato il simbolo normale. All'utente self-service non è consentito modificare il simbolo poiché è di sola lettura.

Per definire aree richiesta/incidente/problema per l'interfaccia self-service

1. Nella scheda Amministrazione, selezionare Service Desk, Richieste/Incidenti/Problemi, Aree.

   Verrà visualizzato l'Elenco aree richiesta/incidente/problema:

2. Fare clic su Modifica in elenco.

   Nella parte superiore della pagina vengono visualizzati i campi modificabili.

3. Aprire l'area incidente/problema/richiesta desiderata per modificarla nell'elenco Simbolo (ad esempio Hardware.pc.install).

4. Inserire i dati nei seguenti campi:

   Includi in self-service

   Specifica se l'area richiesta/incidente/problema è visualizzata nell'interfaccia self-service.

   Simbolo di self-service

   Specifica un identificatore univoco per questa area richiesta/incidente/problema nell'interfaccia self-service.

   Attivo

   Specifica se l'area richiesta/incidente/problema è attiva o non attiva.

   L'area richiesta/incidente/problema è definita per l'interfaccia self-service.

5. Fare clic su Salva.

   Visualizzando di nuovo l'elenco, l'area richiesta/incidente/problema aggiornata viene visualizzata nell'Elenco aree richiesta/incidente/problema.

Categorie Ordine di cambiamento e Issue

Le categorie Cambiamento e Issue definiscono i raggruppamenti logici in cui possono essere organizzati gli Ordini di cambiamento e le Issue.

Nota: a differenza delle aree Richiesta/Incidente/Problema, le categorie Ordine di cambiamento e Issue sono gestite separatamente:

- Impostare le categorie di Cambiamento per i modelli di CA SDM interni e combinati.
- Impostare le categorie di Issue per i modelli di CA SDM esterni e combinati.

Le categorie possono essere utilizzate per specificare i valori predefiniti per specifici campi nei ticket. È possibile associare automaticamente un livello di servizio ai ticket assegnando un tipo di servizio predefinito alle categorie. Inoltre, è possibile associare un'indagine a una categoria.

Per ogni categoria è possibile specificare gli attributi o le qualità da associare al ticket e creare un flusso di lavoro che identifichi tutte le singole attività necessarie alla compilazione del ticket. La definizione dei comportamenti associati alle attività del flusso di lavoro, consente di notificare al personale appropriato l'eventuale modifica dello stato oppure quando le attività chiudono il ticket.

Quando un analista assegna un ticket a una categoria, tutte le informazioni associate alla categoria vengono immesse automaticamente nel ticket. Ad esempio, se si indica un tipo di servizio, questo viene associato al ticket e a tutti gli eventi tipo di servizio associati.

Nota: per ulteriori informazioni sulla definizione e sulla modifica delle categorie, vedere la *Guida in linea*.

Ulteriori informazioni:

Categorie di cambiamento predefinite (a pagina 412)
Categorie di questione predefinite (a pagina 413)
Regole per la modifica delle categorie in un ticket (a pagina 413)
Proprietà delle categorie (a pagina 414)
Definizione di categorie questione e cambiamento per l'interfaccia self-service (a pagina 416)

Categorie di cambiamento predefinite

In CA SDM sono installate le seguenti categorie di cambiamento predefinite:

- Aggiungi
- Modifica
- Sposta
- Ritira

Nota: tutte queste categorie sono suddivise in sottocategorie più specifiche. Ad esempio, la categoria Modifica include categorie per modificare server e workstation.

Categorie di questione predefinite

In CA SDM sono installate le seguenti categorie di questione predefinite:

- Hardware.pc.install
- Software.pc.install

È possibile impostare lo stato di qualsiasi categoria su attivo o non attivo. Disattivando una categoria, non la si elimina dal database ma la si rende indisponibile agli analisti. Se in seguito si decide di utilizzare la categoria, cambiarne di nuovo lo stato su attivo.

Regole per la modifica delle categorie in un ticket

Le regole riportate di seguito interessano solo le attività del flusso di lavoro.

- Se la categoria precedente ha utilizzato CA Workflow o il flusso di lavoro classico e la nuova categoria utilizza CA Process Automation, la definizione del processo CA Process Automation si collega ad un flusso di lavoro in un server CA Process Automation.
- Se la vecchia e la nuova categoria utilizzano il flusso di lavoro di CA SDM, vengono applicate le regole delle versioni precedenti.
- Se la nuova categoria utilizza CA Workflow o CA Process Automation e quella precedente utilizza il flusso di lavoro CA SDM, si verifica quanto segue:
  - Tutte le attività del flusso di lavoro incomplete e in sospeso (ovvero aggiornabili) della versione 6.0 di CA SDM vengono impostate sullo stato annullato indipendentemente dall'opzione KEEP_TASKS. Le attività del flusso di lavoro completate vengono mantenute ma non possono essere riaperte.
  - Vengono eliminate le attività incomplete e non attive, ad esempio quelle in stato di attesa.
  - Viene creata un'istanza della definizione CA Workflow o CA Process Automation.
- Se la nuova categoria utilizza il flusso di lavoro di CA SDM e quella precedente utilizza CA Workflow o CA Process Automation, si verifica quanto segue:
  - L'istanza CA Workflow o CA Process Automation viene impostata sullo stato Interrotto.
  - Le attività del flusso di lavoro della nuova categoria vengono aggiunte normalmente.

- Se entrambe le categorie utilizzano CA Workflow, si verifica quanto segue:
  - Se la vecchia e la nuova categoria puntano alla stessa definizione di processo, l'istanza in esecuzione dalla vecchia categoria prosegue.
  - Se la categoria nuova e quella precedente puntano a definizioni di processo differenti, l'istanza precedente viene impostata su Interrotto e viene creata un'istanza della definizione dalla nuova categoria.

In un flusso di lavoro di CA SDM, non è possibile chiudere un ticket con un'istanza CA Workflow in esecuzione. Le funzioni Accumula, Accelera e Inserisci attività vengono disattivate per i ticket che utilizzano CA Workflow.

Proprietà delle categorie

Le proprietà vengono utilizzate per aggiungere attributi o qualità personalizzati ad una specifica categoria. Se sono state aggiunte delle proprietà a una categoria, quando un analista assegna un ticket a quella categoria, le proprietà associate compaiono automaticamente nella scheda Proprietà del ticket.

Ad esempio, è possibile aggiungere proprietà alla categoria questione predefinita Software.pc.install per specificare dimensione della memoria, tipo di processore e così via.

Quando si definiscono le proprietà è possibile specificare se un valore è richiesto o facoltativo. Per le proprietà con un valore obbligatorio, gli utenti devono immettere un valore o accettare quello predefinito prima di poter salvare il ticket.

Conservazione delle proprietà di una categoria

L'opzione keep_tasks determina ciò che accade se si assegna un ticket esistente ad un'altra categoria:

- Se l'opzione keep_tasks non è installata, le proprietà esistenti e le attività flusso di lavoro vengono rimosse dal ticket e vengono aggiunte tutte le proprietà o le attività associate alla nuova categoria.
- Se l'opzione keep_tasks è installata, le proprietà e le attività esistenti vengono mantenute nel ticket e ad esse vengono aggiunte tutte le proprietà o le attività associate alla nuova categoria.

Nota: per istruzioni dettagliate su come aggiungere le proprietà a una categoria cambiamento o questione e definire le regole di validazione delle proprietà, vedere la *Guida in linea*.

Regole di validazione proprietà

È possibile definire regole di validazione per stabilire una serie di valori predefiniti ai quali possono accedere gli utenti. Ad esempio, se si definisce una proprietà chiamata Sistema operativo, è possibile stabilire una regola di validazione sotto forma di elenco a discesa con le opzioni Windows, UNIX e Linux.

Le proprietà definite senza regole di validazione sono visualizzate come caselle di testo libero, in cui è possibile immettere qualsiasi stringa di testo. Le regole di validazione semplificano il processo di reporting sui valori per aree e categorie e lo rendono meno esposto a errori.

Nota: le regole di validazione delle proprietà sono riutilizzabili. Non sono specifiche di una determinata proprietà. È possibile applicare qualsiasi regola di validazione esistente alle proprietà definite per categorie cambiamento e questione o aree richiesta/incidente/problema.

A seconda del tipo di regola di validazione configurata per una proprietà, quando l'utente assegna un ticket alla categoria o all'area a cui è associata la proprietà, viene visualizzato uno dei controlli seguenti sulla scheda Proprietà del ticket:

- Casella di modifica del testo—Non è stata definita alcuna regola di validazione e non è possibile specificare alcun valore predefinito. Gli utenti devono immettere valori che seguano gli esempio forniti.
- Casella di controllo—Casella di controllo con due stati visualizzata nella scheda Proprietà. Per impostazione predefinita, la casella di controllo non contiene un segno di spunta. L'utente può accettare il valore predefinito o selezionare la casella di controllo. Le caselle che contengono un segno di spunta sono visualizzate sulla pagina Dettagli del ticket, con la dicitura Sì nella colonna del valore. Per le caselle deselezionate nella colonna del valore viene visualizzato No.
- Elenco a discesa—Elenco a discesa contenente un set predefinito di opzioni visualizzato nella scheda Proprietà. Se è stato definito un valore predefinito, viene selezionato quando l'elenco di elenco viene visualizzato la prima volta. L'opzione selezionata dall'utente compare nella colonna del valore nella pagina Dettagli del ticket.

Definizione di categorie questione e cambiamento per l'interfaccia self-service

È possibile utilizzare l'opzione Includi in self-service per definire quali categorie questione e cambiamento includere nei ticket per l'interfaccia self-service. È anche possibile definire simboli di self-service diversi rispetto a quelli visti dall'analista. Al salvataggio del ticket, il simbolo di self-service viene visualizzato nel campo Categoria cambiamento (o questione). Se il ticket viene visualizzato nell'interfaccia dell'analista, per la categoria viene visualizzato il simbolo normale.

Per definire una categoria cambiamento (o questione) per l'interfaccia self-service

1. Nella scheda Amministrazione, selezionare Service Desk, Ordini di cambiamento (o Questioni), Categorie.

   Viene visualizzata la pagina Elenco categorie.

2. Fare clic su Modifica in elenco.

   Nella parte superiore della pagina vengono visualizzati i campi modificabili.

3. Selezionare la categoria desiderata dall'elenco Simbolo.

4. Inserire i dati nei seguenti campi:

   Includi in self-service

   Specifica se la categoria è visualizzata nell'interfaccia self-service.

   Impostazione predefinita: Sì

   Simbolo di self-service

   Specifica un identificatore univoco per questa categoria nell'interfaccia self-service.

   Attivo

   Specifica se la categoria è attiva o non attiva.

   La categoria è definita per l'interfaccia self-service.

5. Fare clic su Salva.

   La categoria aggiornata viene visualizzata nell'Elenco categorie cambiamento (o richiesta) quando si visualizza nuovamente l'elenco.

Chiusura automatica dei ticket

È possibile utilizzare un'impostazione configurabile per consentire la chiusura automatica di ticket (Richieste/Incidenti/Problemi, Ordini di cambiamento o Issue). Quando lo stato di un ticket viene impostato su Risolto, il ticket viene chiuso automaticamente entro il numero di ore lavorative specificate. La notifica attività di Chiusura automatica inviata all'utente finale mostra il numero di ore lavorative rimanenti prima che il ticket venga chiuso. Il numero di ore è configurabile e specifico del titolare. Se lo stato viene modificato prima della scadenza del numero di ore configurabile, la chiusura del ticket viene annullata.

Gli amministratori possono effettuare le seguenti operazioni:

- Definire un'impostazione di chiusura automatica per controllare il numero di ore lavorative, per l'utente finale, prima della chiusura automatica del ticket.
- Impostare una notifica attività di chiusura automatica per informare i contatti interessati circa quando è prevista la chiusura automatica per un ticket.

Nota: se si usa la funzionalità di multi-tenancy, considerare quanto segue:

- Il sistema utilizza l'impostazione pubblica predefinita di chiusura automatica quando non trova un'impostazione di chiusura automatica specifica per il titolare.
- È disponibile un'impostazione di chiusura automatica per ogni titolare.

Nota: per ulteriori informazioni sull'esecuzione di queste procedure, vedere l'argomento relativo alle impostazioni di chiusura automatica nella *Guida in linea*.

Ulteriori informazioni:

Modalità di definizione delle impostazioni di chiusura automatica dei ticket (a pagina 417)
Modalità di definizione di una notifica di attività di chiusura automatica (a pagina 418)

Modalità di definizione delle impostazioni di chiusura automatica dei ticket

È possibile definire il numero di ore lavorative entro le quali un ticket viene chiuso (per tutti i tipi di ticket) come riportato di seguito:

1. Nella scheda Amministrazione, selezionare Service Desk, Dati applicazione, Codici, Chiusura automatica.
2. Fare clic su Crea nuovo nella pagina dell'elenco.
3. Compilare i seguenti campi della pagina dei dettagli:

   Simbolo

   Definisce il nome dell'impostazione di sistema.

Richiesta/Incidente/Problema/Ordine di cambiamento/Questione

Definisce il numero di ore lavorative trascorse le quali il ticket viene impostato sullo stato Risolto prima di venire chiuso. Se lo stato viene modificato prima della scadenza, la chiusura del ticket viene annullata. 0 (zero) ore indica che la chiusura automatica non è implementata per il tipo di ticket.

Descrizione

Fornisce una breve descrizione del record.

Stato

Indica se il record è attivo o non attivo.

L'impostazione di chiusura automatica è definita.

4. Fare clic su Salva e chiudere la finestra.

   La nuova impostazione viene visualizzata nella pagina Elenco impostazioni di chiusura automatica quando si visualizza nuovamente l'elenco.

Modalità di definizione di una notifica di attività di chiusura automatica

È possibile modificare le impostazioni predefinite della notifica di attività di chiusura automatica per informare i contatti appropriati quando per un ticket è pianificato una chiusura automatica. L'attività è valida per tutti i tipi di ticket di CA SDM e include una regola di notifica predefinita per richieste/incidenti/problemi, ordini di cambiamento e questioni.

Per definire una notifica di attività di chiusura automatica, procedere come segue:

1. Nella scheda Amministrazione, selezionare Notifiche, Notifiche attività.
2. Selezionare la notifica di attività Chiusura automatica nella pagina di elenco per aprirla.
3. Aggiornare la regola di notifica Chiusura automatica predefinita e specificare i contatti che riceveranno le notifiche.
4. Fare clic su Salva, quindi su Chiudi finestra.

   Quando visualizzato nuovamente, l'Elenco notifiche attività conterrà la notifica di attività Chiusura automatica aggiornata.

Attività correlate ai ticket

Quando viene generata un'attività per un ticket di <USDK, è possibile propagarla a uno o più ticket correlati. Ad esempio, un record Problema creato da un Incidente può aggiornare il record Incidente una volta risolto il Problema. Quando si verifica l'attività, per il ticket correlato viene generato un registro attività, che include le seguenti informazioni:

- Tipo di attività del ticket correlato, ad esempio Aggiorna stato
- Nome contatto
- Tipo di ticket padre e relativo numero di riferimento
- Descrizione del registro attività, ad esempio stato aggiornato da Operazione in corso ad Aperto

I registri attività vengono propagati a ticket correlati basati sulle proprietà impostate all'interno di ciascuna notifica di attività. Gli attributi dei ticket correlati non vengono modificati. Vengono propagate le seguenti relazioni:

  - I Problemi vengono propagati a tutti gli Incidenti attivi.
  - Gli Ordini di cambiamento vengono propagati a tutti i Problemi e Incidenti attivi.

In qualità di amministratore di sistema è possibile eseguire le seguenti azioni:

- Impostare notifiche di attività per propagare attività a ticket correlati.
- Configurare una notifica attività ticket correlato per notificare i contatti appropriati quando l'attività viene propagata ai ticket correlati.

Nota: per ulteriori informazioni sull'esecuzione di queste procedure, vedere l'argomento relativo alle notifiche di attività nella *Guida in linea*.

Ulteriori informazioni:

Registro attività (a pagina 496)
Modalità di definizione di attività di notifica per ticket correlati (a pagina 420)
Modalità di definizione delle notifiche attività ticket correlati (a pagina 420)

Modalità di definizione di attività di notifica per ticket correlati

È possibile propagare i ticket correlati ai registri attività in base alle proprietà impostate in ognuna di esse. Gli attributi dei ticket correlati non vengono modificati.

Per definire un'attività di notifica per attività di ticket correlati, procedere come segue:

1. Nella scheda Amministrazione, selezionare Notifiche, Notifiche attività.
2. Aprire una notifica attività per modificarla.
3. Nella pagina dei dettagli, selezionare la casella di controllo Attività ticket correlato.

   Nota: se si usa la funzionalità di multi-tenancy, procedere come segue:

   - Nell'elenco a discesa Attività ticket correlato, specificare il tipo di titolare.
   - Immettere il nome del titolare nel campo del titolare o fare clic sull'icona di ricerca per individuarne uno.
4. (Facoltativo) Aggiornare la regola di notifica predefinita e specificare i contatti che riceveranno le notifiche.
5. Fare clic su Salva e chiudere la finestra.

   Quando visualizzato nuovamente, l'Elenco Notifiche attività conterrà la notifica attività aggiornata.

Modalità di definizione delle notifiche attività ticket correlati

È possibile modificare le impostazioni predefinite nella notifica attività ticket correlato per informare i contatti interessati quando i registri attività vengono propagati a ticket correlati (richieste/incidenti/problemi, ordini di cambiamento e questioni).

Per definire una notifica attività ticket correlato, procedere come segue:

1. Aprire la notifica attività Ticket correlati nella pagina Elenco notifiche attività.
2. Fare clic su Modifica e modificare uno o più campi, in base alle esigenze, nella pagina dei dettagli.
3. (Facoltativo) Aggiornare la regola di notifica predefinita e specificare i contatti che riceveranno le notifiche.
4. Fare clic su Salva e chiudere la finestra.

   Quando visualizzato nuovamente, l'Elenco Notifiche attività conterrà la notifica attività del ticket correlato aggiornata.

Calcolo della priorità

Il *calcolo della priorità* corrisponde a un insieme predefinito di valori che imposta automaticamente i campi Priorità, Urgenza e Impatto di Problemi e Incidenti. Il calcolo della priorità aiuta a gestire gli Incidenti e i Problemi in base alle esigenze dell'azienda e alle strutture IT disponibili. ITIL consiglia di assegnare una priorità ai ticket utilizzando un processo di calcolo dei dati basato sui valori di Urgenza e Impatto. Le organizzazioni di supporto definiscono questo calcolo in base ai processi specifici in uso, alla modalità di definizione degli accordi sui livelli di servizio (SLA) e altri eventi chiave del sistema. Inoltre è possibile includere in questo calcolo il livello di criticità degli elementi della configurazione collegati all'Incidente e al Problema. Assegnare le priorità ai ticket consente di realizzare quanto segue:

- Allocare le risorse IT per i ticket
- Fornire un servizio migliore ai clienti
- Ridurre costi

La soluzione di CA SDM per il calcolo delle priorità include i seguenti componenti:

- Una matrice di calcolo priorità basata sui valori Urgenza e Impatto,
- Valori predefiniti per Urgenza e Impatto
- Opzioni di modifica per Urgenza e Impatto basate su Servizio interessato, Data di apertura, Utente finale interessato e Area Incidente o Problema
- Un'opzione Motivo acquisizione per modificare manualmente Urgenza o Impatto
- Un'opzione Abilita per Modelli per creare un ticket da un modello

Quando si installa CA SDM, i valori dei ticket vengono automaticamente gestiti da un calcolo della priorità predefinito. È possibile modificare le impostazioni del calcolo della priorità oppure creare calcoli della priorità aggiuntivi per gestire gli Incidenti o i Problemi. Nel calcolo della priorità è possibile definire il risultato in base agli scenari di business per una maggiore coerenza dei livelli di importanza e della gestione dei ticket. Sebbene gli utenti possano ignorare alcune impostazioni, la priorità del ticket non può essere modificata in quanto viene definita automaticamente in base ai dati. In Multi-Tenancy, l'utente o i titolari possono creare calcoli della priorità aggiuntiva configurando impostazioni specifiche per ciascun titolare.

Quando un analista apre un Incidente o un Problema, il sistema usa automaticamente un calcolo della priorità attivo e i valori del ticket per generare le impostazioni Priorità, Urgenza e Impatto. Le impostazioni sono basate su uno o più dei seguenti campi:

- Urgenza
- Impact
- Utente finale interessato
- Area Incidente o Problema
- Data di apertura
- Servizio interessato

Gli analisti possono ignorare i valori Urgenza e Impatto, se necessario. In base alla configurazione di Gestione opzioni, i dipendenti possono ignorare solo i valori Urgenza di Incidenti quando è installata l'opzione *urgency_on_employee*. Se il flag Motivo acquisizione è attivato e gli utenti ignorano i valori Urgenza o Impatto e selezionano Salva, viene visualizzata la pagina dei dettagli dell'escalation in cui gli utenti possono immettere il motivo del cambiamento.

Tutti i calcoli priorità dei ticket, le modifiche manuali e le informazioni sul motivo compaiono nel Nuovo registro attività. Se non il calcolo della priorità non viene modificato, il sistema non crea una voce del registro attività.

Nota: in caso di migrazione da una versione precedente, il calcolo della priorità è disattivato per impostazione predefinita. Per informazioni sulla modalità di attivazione del calcolo della proprietà o il mantenimento delle impostazioni personalizzate, consultare la *Guida all'implementazione*.

Modalità di gestione dei valori dei ticket da parte del calcolo della priorità

Il sistema modifica i valori di problemi e incidenti in base alle impostazioni del calcolo della priorità attivo per consentire agli analisti di gestire i ticket in modo più efficiente. La tabella riportata illustra come il calcolo della priorità modifica i campi in base al calcolo priorità e alle azioni dell'utente per problemi, incidenti, servizio Web, posta elettronica e API testo:

Azione	Modifica automatica campi	Descrizione
L'utente modifica il Servizio interessato	Impatto Priorità	Il sistema valuta il valore Impatto del servizio nell'elemento della configurazione di tipo Servizio per calcolare il nuovo valore Impatto. Gli elementi della configurazione di tipo Servizio sono definiti come elementi della configurazione con la relativa classe definita nella famiglia Servizio Enterprise. Se la data di apertura del ticket si trova all'interno di un periodo definito da una finestra di blackout, il sistema incrementa il nuovo valore Impatto in base al campo Incremento impatto. Il sistema sostituisce solo il valore Impatto quando il nuovo valore è maggiore del valore Impatto iniziale.
L'utente modifica l'Area incidente.	Urgenza	Il valore Urgenza viene modificato solo se il nuovo valore è maggiore del valore predefinito.
L'utente modifica l'Area incidente *e* l'Utente finale interessato	Urgenza Priorità	Se l'utente imposta l'Area incidente per prima, il valore Urgenza verrà modificato dopo aver impostato l'Utente finale interessato. Il calcolo della priorità imposta il valore della priorità.

Azione	Modifica automatica campi	Descrizione
L'utente modifica Urgenza *e* Impatto	Priorità Impatto	Il sistema valuta il valore Impatto del servizio nell'elemento della configurazione di tipo Servizio per calcolare il nuovo valore Impatto. Se la data di apertura del ticket si trova all'interno di un periodo definito da una finestra di blackout, il sistema incrementa il nuovo valore Impatto in base al campo Incremento impatto. Il sistema sostituisce solo il valore Impatto quando il nuovo valore è maggiore del valore Impatto iniziale. Se l'amministratore imposta l'opzione Motivo acquisizione, l'utente dovrà specificare il motivo della modifica. Se l'utente cambia i valori Urgenza o Impatto, tali valori rimangono invariati durante l'intera creazione o aggiornamento del ticket finché l'utente non li modifica nuovamente. Tuttavia, il sistema può aggiornare i valori ignorati Urgenza o Impatto la volta successiva che l'utente aggiorna il ticket. Dopo che il sistema modifica i valori Urgenza e Impatto, il calcolo della priorità imposta il valore Priorità.
L'utente seleziona Nuovo incidente in base al Documento della conoscenza e prevalgono i valori dei Documenti della conoscenza (a pagina 432)	Impatto Urgenza	Il sistema utilizza sempre i valori del Documento della conoscenza o della soluzione della conoscenza indipendentemente dal fatto che essi siano maggiori o minori dei valori predefiniti del calcolo della priorità. Ad esempio, se un calcolo della priorità ha un valore Impatto pari a 3-Gruppo singolo e Urgenza pari a 3-Rapidamente, e i Documenti della conoscenza hanno un valore Impatto pari a 2-Più gruppi e Urgenza 4-Molto rapidamente, il sistema applica all'incidente i valori dal Documento della conoscenza. Il valore Priorità viene sempre ottenuto dal calcolo della priorità.
L'utente accetta il Documento della conoscenza come soluzione al problema o all'incidente	Impatto Urgenza	Il sistema utilizza i valori dal Documento della conoscenza per Impatto e Urgenza. Il sistema utilizza anche il calcolo della priorità per impostare il valore Priorità.
L'utente deriva l'incidente dal Documento della conoscenza selezionando Nuovo incidente	Impatto Urgenza Priorità	Il sistema utilizza i valori del calcolo della priorità.

Azione	Modifica automatica campi	Descrizione
L'utente acquisisce l'Incidente dal Documento della conoscenza senza la sovrascrittura dei valori dei Documenti della conoscenza (a pagina 432)	Impatto Urgenza Priorità	Il sistema utilizza i valori del calcolo della priorità indipendentemente dalla modalità con cui l'utente ha creato l'incidente per il Documento della conoscenza o la soluzione della conoscenza.
Il ticket accetta il Documento della conoscenza come soluzione al problema o all'incidente e i valori dei documenti della conoscenza non prevalgono	Impatto Urgenza Priorità	Il sistema utilizza valori da un problema o incidente. Il valore Priorità deriva dal calcolo della priorità.
I ticket in modalità sola lettura accettano il Documento della conoscenza come soluzione al problema o all'incidente e prevalgono i valori dei Documenti della conoscenza	Impatto Urgenza Priorità	Il sistema utilizza i valori Impatto e Urgenza dal Documento della conoscenza nel caso in cui i valori non siano vuoti. Se il valore Impatto/Urgenza del Documento della conoscenza è vuoto, il sistema utilizza i valori del Problema o dell'Incidente. Il valore Priorità deriva dal calcolo della priorità.
Il ticket in modalità modifica accetta il Documento della conoscenza come soluzione al problema o all'incidente e prevalgono i valori dei Documenti della conoscenza	Impatto Urgenza Priorità	Il sistema utilizza valori del Problema o Incidente. Il valore Priorità deriva dal calcolo della priorità.

Generazione del valore di urgenza dopo il salvataggio del ticket mediante il calcolo della priorità

Il calcolo della priorità genera i valori di urgenza solo in seguito al salvataggio degli Incidenti da parte degli utenti self-service. Tali utenti, ad esempio i dipendenti VIP, i dipendenti e gli utenti anonimi, possono visualizzare il valore generato dopo aver salvato il ticket.

Per gli utenti self-service, il calcolo della priorità utilizza le impostazioni e i valori seguenti per generare i valori di urgenza:

- Urgency_On_Employee impostato su Sì in Gestione opzioni
- Il valore Sovrascrivi urgenza è abilitato nel calcolo della priorità attivo per gli Incidenti
- Le impostazioni di urgenza *Web.cfg* quali AnonymousUrg per gli utenti anonimi, ESCEmpUrg per i dipendenti VIP e EmpUrg per tutti gli altri dipendenti

- Valori dell'area urgenza
- Sovrascrittura manuale da parte dell'utente

La tabella seguente contiene un riepilogo della procedura di impostazione del valore di urgenza mediante il calcolo della priorità per gli Incidenti self-service:

Azione dell'utente self-service	Valore dell'urgenza
L'utente salva un Incidente con il valore di urgenza predefinito e un'Area Incidente vuota.	Il ticket mostra il valore Urgenza predefinito di *web.cfg*.
L'utente salva un Incidente dopo aver sovrascritto il valore Urgenza.	Indipendentemente dalle impostazioni di Urgenza area, *web.cfg* o calcolo priorità, il ticket mostra il valore Urgenza selezionato dall'utente.
L'utente salva un incidente dopo aver selezionato un'Area Incidente. L'Area Incidente non presenta un valore predefinito per Urgenza area.	Il ticket mostra il valore Urgenza predefinito di *web.cfg*.
L'utente salva un incidente dopo aver selezionato un'Area Incidente con un valore Urgenza Area predefinito. L'opzione Sovrascrivi urgenza è abilitata anche nel calcolo priorità attivo per gli incidenti.	Se il valore Urgenza area è maggiore del valore Urgenza nel file *web.cfg*, il ticket mostra il valore Urgenza area. Il campo Urgenza aggiornato non è tuttavia visibile mentre l'utente crea o modifica il ticket. Quando l'utente salva e riapre l'incidente, sull'incidente viene visualizzato il valore Urgenza aggiornato.
L'utente salva un incidente dopo aver selezionato un'Area Incidente con un valore Urgenza Area predefinito. L'opzione Sovrascrivi urgenza è tuttavia disabilitata nel calcolo priorità attivo per gli incidenti.	Il ticket mostra il valore Urgenza di *web.cfg*.
L'utente modifica un incidente esistente con un'Area Incidente che presenta un valore Urgenza Area predefinito.	L'elenco a discesa Urgenza mostra il valore Urgenza area e tutti i valori di *web.cfg* applicabili.

Nota: per informazioni sull'impostazione dei valori di urgenza per gli utenti self-service, consultare la *Guida all'implementazione*.

Modalità di impostazione del calcolo della priorità

Per impostazione predefinita, valori di ticket quali il valore Priorità sono basati su un calcolo della priorità. È possibile trovare e modificare i valori iniziali di Priorità e Urgenza nel file web.cfg. Il file web.cfg include impostazioni separate per tipologia di utente, ad esempio utente guest, utente VIP e dipendente.

Nota: in caso di aggiornamento da una versione precedente, il calcolo della priorità è disattivato per impostazione predefinita. Le pagine personalizzate Dettagli incidente e problema richiedono un'ulteriore configurazione per operare in modo corretto. Per informazioni sulla modalità di attivazione del calcolo della proprietà o per mantenere le personalizzazioni, consultare la *Guida all'implementazione*.

Per impostare il calcolo della priorità, procedere come segue:

1. Nella scheda Amministrazione, selezionare Service Desk, Richieste/Incidenti/Problemi, Calcolo priorità.

   Viene visualizzato l'elenco Calcolo priorità.

2. Fare clic con il pulsante destro del mouse sul calcolo della priorità predefinito e selezionare Modifica dal menu di scelta rapida.

   Viene visualizzata la pagina Dettagli calcolo priorità che mostra le impostazioni predefinite per i ticket incidente e problema.

3. Rivedere il calcolo della priorità predefinito e modificare i valori secondo necessità. Quando si impostano valori per il calcolo della priorità, considerare le seguenti implicazioni relative all'ambiente di lavoro:

   - **Escalation delle questioni**—Quando i ticket richiedono un'escalation a un determinato VIP, è possibile aumentare il valore Urgenza.
   - **Elementi della configurazione critici**—Per gli elementi della configurazione critici è possibile configurare il valore Impatto del servizio per ogni elemento della configurazione.
   - **Tempo di attività di servizi critici**—Quando un elemento della configurazione richieste la massima disponibilità, aggiungere una finestra di blackout.
   - **Finestra di blackout**—Quando ticket relativi a elementi delle configurazione utilizzano una determinata finestra di blackout, è possibile aumentare il valore Impatto del servizio nel calcolo della priorità.

4. Utilizzare l'impostazione di sovrascrittura manuale per consentire agli utenti di modificare i ticket in base alle specifiche esigenze.

5. Se si desidera un calcolo della priorità separato per la gestione di problemi o incidenti, configurare il tipo di ticket (a pagina 430).

6. Fare clic su Salva.

   Nel successivo ticket o documento della conoscenza, nuovo o aggiornato, i campi si aggiornano in base ai valori specificati nel calcolo priorità attivo.

7. Considerare l'eventuale creazione di calcoli della priorità aggiuntivi per ogni tipo di ticket. In installazioni multi-tenancy, creare e attivare calcoli della priorità aggiuntivi per gestire i ticket di ciascun titolare.

Nota: per informazioni sul calcolo della priorità, consultare la *Guida in linea*.

Calcoli della priorità multipli

È possibile impostare più calcoli della priorità, Tuttavia, un solo calcolo della priorità attivo gestisce problemi, incidenti oppure entrambi. Ad esempio, è possibile disporre di un calcolo della priorità attivo per i problemi e un altro per gli incidenti. È inoltre possibile salvare vari calcoli della priorità non attivi per l'uso futuro.

Assegnazione del calcolo priorità per l'opzione multi-tenancy

L'utente o i relativi titolari possono creare calcoli di priorità specifici dei titolari per gestire incidenti e problemi. Quando si assegnano calcoli di priorità per l'opzione multi-tenancy, prendere in considerazione quanto segue:

- Quando un calcolo priorità non dispone di titolari assegnati, viene considerato pubblico. Lo stato del calcolo di una priorità pubblica può essere Attivo o Inattivo. Un calcolo priorità non è più considerato pubblico quando viene assegnato a un titolare.

- Se un titolare non dispone di un'assegnazione calcolo priorità, il calcolo priorità Predefinito o un altro calcolo priorità pubblico attivo gestirà automaticamente problemi e incidenti.

- Un calcolo priorità gestisce problemi e incidenti per un titolare. Tuttavia, un calcolo priorità separato specifico del titolare può gestire ciascun tipo di ticket. Ad esempio, l'azienda X dispone di un calcolo priorità per gestire incidenti e un altro per gestire i problemi.

- Quando i titolari creano i propri calcoli priorità mentre i calcoli priorità pubblici sono attivi, il calcolo priorità specifico del titolare verrà applicato solo ai ticket per il rispettivo titolare.

  Ad esempio, se il calcolo priorità Predefinito è attivo, il titolare dell'azienda X potrà creare un calcolo priorità specifico del titolare denominato new_priority_calculation. Le nuove impostazioni e configurazioni di new_priority_calculation si applicano solo a incidenti e problemi dell'azienda X.

- Se il titolare disattiva un calcolo priorità, il sistema utilizza un calcolo priorità pubblico attivo per gestire i problemi e gli incidenti del titolare.

  Ad esempio, l'azienda X disattiva il calcolo priorità specifico del titolare mentre esiste ancora un calcolo priorità Predefinito attivo. Il calcolo priorità rimane attivo per l'azienda X perché il sistema utilizza il calcolo priorità Predefinito per gestire incidenti e problemi dell'azienda X.

  Nota: poiché i titolari possono eliminare i propri record di calcolo priorità, vi consigliamo di disattivare i calcoli di priorità pubblici che gestiscono incidenti e problemi. Invece, l'utente o i titolari possono creare calcoli priorità specifici del titolare.

- Quando si disattiva l'opzione multi-tenancy ed è presente più di un calcolo priorità attivo che gestisce i titolari, lasciare *solo un* calcolo priorità per gestire incidenti e problemi. Ad esempio, è possibile disattivare tutti i calcoli priorità eccetto uno per gestire incidenti e un altro per gestire i problemi.

Nota: per ulteriori informazioni sull'opzione multi-tenancy, consultare la *Guida all'implementazione*.

Modalità di assegnazione di un titolare a un calcolo priorità

Per l'opzione multi-tenancy è possibile assegnare un titolare a un calcolo priorità. Innanzitutto è necessario disattivare i calcoli priorità pubblici. Quindi è necessario assegnare il titolare a un calcolo priorità ed attivarlo.

Per assegnare un titolare a un calcolo priorità, effettuare una delle operazioni seguenti:

1. Nella scheda Amministrazione, selezionare Service Desk, Richieste/Incidenti/Problemi, Calcolo priorità.

   Viene visualizzato l'elenco Calcolo priorità.

2. Modificare ciascun calcolo priorità pubblico, come Predefinito. Impostare lo stato su Non attivo e fare clic su Salva.

   Il sistema disattiva i calcoli priorità pubblici.

3. Per ciascun titolare, creare o modificare un calcolo priorità con impostazioni specifiche per il titolare per Impatto, Urgenza e Priorità.

   Viene visualizzata la pagina per la creazione o l'aggiornamento del calcolo priorità.

4. Nel campo Nome, immettere il titolare.

5. Nel campo Stato selezionare Attivo.

6. Fare clic su Salva.

   Il sistema applica i valori specifici per il titolare a Impatto, Urgenza e Priorità nei nuovi incidenti e problemi.

Nota: per informazioni sulla creazione e la modifica dei calcoli priorità, vedere la *Guida in linea*.

Considerazioni sui tipi di ticket per il calcolo della priorità

Quando si configurano tipi di ticket per il calcolo della priorità, considerare quanto riportato di seguito:

- Il calcolo della priorità predefinito consente di gestire entrambi i tipi di ticket, problema e incidente.
- Se si sta effettuando l'aggiornamento da una versione precedente, è possibile attivare il calcolo della priorità predefinito oppure creare una calcolo della priorità per gestire problemi e incidenti.
- Sebbene siano consentiti più calcoli della priorità, solo un calcolo della priorità attivo può gestire un determinato tipo di ticket. Ad esempio, un calcolo della priorità attivo può gestire problemi e un altro può gestire incidenti.
- Se si desidera creare un calcolo della priorità e un calcolo della priorità attivo già gestisce un determinato tipo di ticket, è innanzitutto necessario disattivare il tipo di ticket nel calcolo della priorità attivo. Ad esempio, se si desidera che un calcolo della priorità gestisca i problemi, è innanzitutto necessario disattivare il tipo di ticket problema nel calcolo della priorità attivo e quindi creare un calcolo della priorità attivo che gestisca i problemi.

Nota: per informazioni sull'attivazione di un calcolo della priorità e sull'impostazione di tipi di ticket durante la migrazione, consultare la *Guida all'implementazione*.

Configurazione di tipi di ticket per il calcolo della priorità

È possibile specificare i tipi di ticket gestiti dal calcolo della priorità. Quando è attivo, il calcolo della priorità gestisce i valori Priorità, Impatto e Urgenza dei nuovi ticket.

Per configurare tipi di ticket per il calcolo della priorità

1. Nella scheda Amministrazione, selezionare Service Desk, Richieste/Incidenti/Problemi, Calcolo priorità.

   Viene visualizzato l'elenco Calcolo priorità.

2. Fare clic con il pulsante destro del mouse su calcolo della priorità e selezionare Modifica.

   Viene visualizzata la pagina Aggiorna calcolo priorità.

3. Selezionare o deselezionare una o più delle seguenti opzioni:

   Incidenti

   Attiva o disattiva il calcolo della priorità per la gestione di nuovi incidenti.

   Problemi

   Attiva o disattiva il calcolo della priorità per la gestione di nuovi ticket problema.

4. Fare clic su Salva.

   Queste impostazioni vengono utilizzate nel calcolo della priorità per gestire i valori di ticket per nuovi incidenti, problemi o entrambi.

Utilizzo dei modelli di ticket per il calcolo dei valori di priorità

Se si desidera utilizzare i modelli di ticket per il calcolo della priorità, configurare il calcolo della priorità con l'opzione *Abilita per modelli*. Se si attiva questa opzione i valori Urgenza e Impatto vengono recuperati dal modello, ma il campo Priorità deriva al record del calcolo della priorità. Il valore della priorità viene visualizzato in sola lettura.

Se non si attiva questa opzione, i valori dei campi Urgenza, Impatto e Priorità provengono dal modello. È possibile modificare il campo Priorità e non viene eseguito alcun calcolo della priorità per il ticket finché quest'ultimo non viene salvato.

Per utilizzare modelli di ticket per calcolare valori di priorità

1. Nella scheda Amministrazione, selezionare Service Desk, Richieste/Incidenti/Problemi, Calcolo priorità.

   Viene visualizzato l'elenco Calcolo priorità.

2. Selezionare il calcolo della priorità desiderato da utilizzare per il calcolo della priorità con modelli.

   È inoltre possibile creare un calcolo della priorità per utilizzare modelli di ticket per calcolare valori di priorità.

3. Selezionare *Attiva da modelli* dell'elenco Opzioni calcolo priorità.

4. Fare clic su Salva.

   L'opzione viene attivata.

Utilizzo di documenti della conoscenza per calcolare valori di priorità

Se si desidera che documenti della conoscenza calcolino la priorità, è possibile aggiornare il mapping dei campi. Dopo aver configurato il mapping dei campi, l'analista può creare ticket incidente o problema da documenti della conoscenza. Il documento della conoscenza calcola i valori Impatto e Urgenza dei ticket. Se manca il valore Impatto o Urgenza, i valori vengono generati dal calcolo della priorità.

Importante Se si modifica e salva un ticket che contiene già valori Impatto e Urgenza calcolati da un documento della conoscenza, il calcolo della priorità prevale sui valori impostati da Gestione della conoscenza. Queste attività sono visualizzate nel registro di controllo.

Per utilizzare documenti della conoscenza per calcolare valori di priorità

1. Nella scheda Amministrazione, selezionare Conoscenza, Integrazione Service Desk.
2. Selezionare Mapping campi.

   Viene visualizzata la pagina Mapping campi.

3. Per le opzioni Impatto e Urgenza, selezionare le caselle di controllo appropriate:

   Inserisci valori Service Desk non specificati

   Specifica se utilizzare le informazioni di Gestione della conoscenza per compilare i campi nelle questioni o nelle richieste.

   Sovrascrivi valori Service Desk

   Identifica i campi in problemi o richieste che corrispondono a campi elencati nella colonna Gestione della conoscenza.

   Nota: quando il campo Sovrascrivi valori Service Desk non è abilitato ma è invece abilitato il campo Inserisci valori Service Desk non specificati per le opzioni Impatto e Urgenza, i valori della conoscenza di Impatto e Urgenza sovrascrivono i valori di Incidente.

4. Fare clic su Salva.

   Gli incidenti e i problemi vengono creati utilizzando i valori Impatto e Urgenza dal documento della conoscenza per calcolare il valore Priorità. Se mancano i valori, il ticket li ottiene da un calcolo della priorità attivo. Se per un tipo di ticket non sono disponibili calcoli della priorità attivi, il sistema cancella i campi Priorità, Urgenza e Impatto.

Sovrascrittura manuale del valore Impatto

Quando si sovrascrive manualmente il valore Impatto di un problema o incidente, il calcolo della priorità attivo che gestisce il tipo di ticket imposta automaticamente il valore Priorità.

Per sovrascrivere manualmente il valore Impatto

1. Aprire la pagina dei dettagli del problema o dell'incidente da modificare.
2. Modificare il valore Impatto.

   Se esiste un calcolo di priorità attivo che gestisce il tipo di ticket, il valore Priorità cambia automaticamente in base alle impostazioni nel calcolo della priorità.

3. Salvare l'incidente.

   Il registro attività nella pagina Dettagli incidente rispecchia le modifiche del valore Impatto.

Esempio: sovrascrittura manuale del valore Impatto di un nuovo incidente

1. Creare un incidente.

   Per impostazione predefinita il valore Urgenza è 3-Rapidamente. Il valore Impatto è 3-Gruppo singolo. Il valore Priorità è 3.

2. Sovrascrivere il valore Impatto su 1-Intera organizzazione.

   Il valore Priorità cambia automaticamente in base ai valori nel calcolo della priorità attiva che gestisce gli incidenti.

3. Salvare l'incidente.

   Il registro attività nella pagina Dettagli incidente rispecchia le modifiche del valore Impatto.

Sovrascrittura manuale del valore Urgenza

Quando si sovrascrive manualmente il valore Urgenza di ticket, il calcolo della priorità attivo che gestisce il tipo di ticket imposta automaticamente il valore Priorità.

Per sovrascrivere manualmente il valore Urgenza

1. Aprire la pagina dei dettagli dell'incidente da modificare.
2. Modificare il valore Urgenza.

   Se esiste un calcolo di priorità attivo che gestisce il tipo di ticket, il valore Priorità cambia automaticamente in base alle impostazioni nel calcolo della priorità.

3. Salvare l'incidente.

   Il registro attività nella pagina Dettagli incidente rispecchia le modifiche del valore Urgenza.

Esempio: sovrascrittura manuale del valore Urgenza di un nuovo incidente

1. Creare un incidente.

   Per impostazione predefinita il valore Urgenza è 3-Rapidamente. Il valore Impatto è 3-Gruppo singolo. Il valore Priorità è 3.

2. Sovrascrivere il valore Urgenza su 5-Immediato.

   Il valore Priorità cambia automaticamente in base ai valori nel calcolo della priorità attiva che gestisce gli incidenti.

3. Salvare l'incidente.

   Il registro attività della pagina Dettagli incidente rispecchia le modifiche del valore Urgenza.

Impostazione automatica dell'impatto per un problema o un incidente

Per gli elementi della configurazione definiti con una famiglia Servizio Enterprise, è possibile impostare automaticamente il valore Impatto per problemi o incidenti. Quando si seleziona l'Area problema o incidente e si seleziona un Servizio interessato, l'impatto viene impostato in base alle impostazioni dell'impatto del servizio degli elementi della configurazione Servizio Enterprise e al calcolo della priorità.

Per impostare automaticamente l'impatto per un problema o un incidente

1. Creare un problema o un incidente per un elemento della configurazione di tipo Servizio Enterprise.

2. Selezionare un Servizio interessato.

3. Selezionare un'area Problema o Incidente.

   Se esiste un calcolo della priorità attivo che gestisce il tipo di ticket, il valore Impatto cambia in base al valore Incremento impatto (utilizzato per la valutazione dell'impatto Finestra blackout) nel calcolo della priorità e al valore Impatto del servizio proveniente dal servizio interessato.

   Se si utilizza il calcolo della priorità predefinito, con un Impatto del servizio per l'elemento della configurazione Servizio Enterprise impostato su 1-Intera organizzazione, e il problema o l'incidente non è aperto all'interno di una Finestra blackout, il valore Impatto nel problema o nell'incidente è impostato su 1 e il valore Priorità sul ticket sale a 2.

4. Salvare il ticket.

   Il registro attività nella pagina Dettagli incidente rispecchia le modifiche del valore Impatto.

Esempio di impostazione dell'impatto per un problema o un incidente

L'esempio riportato di seguito illustra come impostare il valore Impatto per un problema o un incidente.

1. Creare un elemento della configurazione Servizio Enterprise denominato EC-APC e impostarne la classe su una delle classi della famiglia Servizio Enterprise.

   Ad esempio, è possibile impostare la classe su Altri servizi, Servizio di business o Servizio per le infrastrutture.

2. Nella scheda Servizio del modulo Dettagli elemento della configurazione, impostare il campo Impatto del servizio su 2-Più gruppi.

3. Nella scheda Service Desk, creare un incidente e impostare il campo Servizio interessato su EC-APC.

4. Salvare il ticket.

   Il campo Impatto dell'incidente rispecchia il valore impostato per Impatto del servizio del servizio interessato selezionato (EC-APC). In questo caso, il valore Impatto è impostato su 2 -Più gruppi.

   Nota: se si utilizza il calcolo della priorità predefinito e il ticket corrente viene creato durante una finestra di blackout, il valore Impatto aumenta di 1 e in questo caso il valore Impatto citato in precedenza viene impostato su 1-Intera organizzazione.

Nota: per informazioni sulla creazione di elementi della configurazione, consultare la Guida in linea.

Impostazione automatica dell'urgenza per un problema o un incidente

Per i problemi e gli incidenti è possibile impostare automaticamente i valori Urgenza e Priorità specificando un utente finale interessato che richiede una Gestione speciale oppure specificando un'Area problema/incidente con un valore Urgenza area.

Quando si assegna a un contatto la gestione speciale, con l'opzione Segnala urgenza attivata, oppure si imposta un'Urgenza area per un'area Problema/Incidente, il valore Urgenza nel problema/incidente viene impostato automaticamente sui valori specificati nel calcolo della priorità e sul valore Urgenza area relativo all'utente finale interessato.

Per impostare automaticamente l'urgenza per un problema o un incidente

1. Creare un problema o un incidente.
2. Selezionare un utente finale interessato. In caso di forte urgenza, selezionare un utente finale interessato che richiede una Gestione speciale con l'opzione Segnala urgenza attivata.

   Se esiste un calcolo della priorità attivo che gestisce il tipo di ticket, il valore Urgenza cambia automaticamente in base al valore Incremento urgenza specificato nel calcolo della priorità attivo.
3. Selezionare un'area Problema o Incidente.

   Se esiste un calcolo della priorità attivo che gestisce il tipo di ticket, il valore Urgenza cambia automaticamente in base al valore Urgenza area specificato nella definizione dell'area Problema/Incidente.
4. Salvare il ticket.

   Un messaggio di conferma ricorda che il ticket necessita di gestione speciale. Il Registro attività della pagina Dettagli problema/incidente rispecchia le modifiche del valore Urgenza.

Esempio di impostazione dell'urgenza per un problema o un incidente

L'esempio riportato di seguito illustra come impostare il valore Urgenza per un problema o un incidente:

1. Nella scheda Amministrazione, creare un contatto denominato Non VIP.
2. Creare un contatto di gestione speciale denominato VIP con l'opzione Segnala urgenza attivata.
3. Creare un'area denominata Area test e specificare l'Urgenza area come 2-Molto rapidamente.
4. Nella scheda Service Desk, creare un incidente.
5. Per Utente finale interessato, selezionare Non VIP.
6. Nell'Area incidente, selezionare Area test e salvare il ticket.

   Il campo Urgenza rispecchia il valore Urgenza area specificato nella definizione Area incidente. In questo caso, l'Urgenza è impostata su 2-Molto rapidamente.
7. Modificare l'utente finale interessato su VIP e salvare il ticket.

   Se si utilizza la matrice di calcolo della priorità predefinita, il valore Urgenza viene aumentato di 1 e impostato su 1-Immediato. Viene visualizzato un messaggio di conferma che ricorda che il ticket necessita di gestione speciale. Il registro attività nella pagina Dettagli incidente rispecchia le modifiche del valore Urgenza.

Nota: per informazioni sulla creazione di contatti e aree, consultare la *Guida in linea*.

Controlli di attributo dipendenti e transizioni di stato

È possibile utilizzare i seguenti controlli configurabili per limitare i flussi di stato dei ticket per Ordini di cambiamento, Issue, Incidenti/Problemi/Richieste, nonché determinare quali campi sono visualizzati o richiesti per ciascun stato di ticket:

Transizioni

Controlla il modo in cui gli utenti selezionano gli stati disponibili nei moduli relativi a Incidente/Problema/Richiesta, Issue o Ordine di cambiamento. Ad esempio, lo stato di un problema è impostato su Aperto e il flusso delle transizioni consente all'analista soltanto di aggiornare lo stato a Chiuso. In questo esempio l'analista non ha a disposizione altre opzioni, il che rinforza il processo di gestione del problema.

Le transizioni consentono di definire un sottoinsieme dell'intero elenco di stati e specificare il nuovo (o successivo) stato predefinito di un ticket in base allo stato corrente. È possibile definire transizioni di stato specifiche per ogni tipo di ticket. Prendere in considerazione l'uso di transazioni quando si desidera limitare i flussi di lavoro dello stato per i propri utenti finali.

Attributi dipendenti

Controllano in che modo gli attributi vengono designati come richiesti (specificazione obbligatoria) o bloccati (impossibile aggiornare), a seconda dello stato del ticket. Ad esempio, il ruolo Gestione Cambiamento può impedire a un'analista di modificare l'attributo Riepilogo dopo l'approvazione di un Ordine di cambiamento. Prendere in considerazione l'uso di controlli di attributo quando si desidera limitare certi attributi in base allo stato.

Nota: è possibile specificare in che misura il sistema forza le norme Stato configurando l'opzione Violazioni norma stato in Gestione opzioni (Opzioni generali). Questa opzione si applica solo ai processi di sistema automatizzati, come le integrazioni e le macro.

Ulteriori informazioni:

Modalità di lavoro con controlli di attributo dipendenti e transizioni di stato (a pagina 438)
Configurazione di transizioni di stato (a pagina 439)
Procedura ottimale: Transizioni di stato predefinite (a pagina 446)

Modalità di lavoro con controlli di attributo dipendenti e transizioni di stato

Per utilizzare controlli di attributo dipendenti e transizioni di stato, procedere come segue:

1. Nella scheda Amministrazione, configurare i titolari, i contatti e i ruoli appropriati per l'ambiente.
2. Nel nodo Service Desk, specificare un tipo di ticket (ad esempio, Ordine di cambiamento) e selezionare Stato.

   Nella pagina Elenco stati vengono visualizzati i codici di stato attivi.
3. Modificare il codice di stato appropriato (ad esempio, Riconosciuto) e utilizzare i controlli disponibili nelle schede nella parte inferiore della pagina dei dettagli dello stato del ticket per effettuare le seguenti operazioni:
   - Configurazione di transizioni di stato (a pagina 439)
   - Configurazione di controlli di attributo dipendenti (a pagina 440)

Nota: è possibile configurare singole transizioni e controlli di attributo dipendenti per ogni tipo di ticket.

Configurazione di transizioni di stato

È possibile definire un sottoinsieme dell'intero elenco di stati e specificare il successivo stato predefinito di un ticket in base allo stato corrente. Le transizioni vengono attuate quando cambia lo stato nel modulo Dettagli ticket.

Per configurare transizioni di stato

1. Fare clic sulla scheda Transizioni nella parte inferiore della pagina Dettagli stato del ticket.

   Nella pagina Elenco transizioni vengono visualizzate tutte le transizioni valide per lo stato.

   Nota: quando sono state configurati, i tipi di transizione collegati vengono visualizzati nell'Elenco transizioni incidente e richiesta.

2. Fare clic sul pulsante Aggiorna transizioni.

   Viene visualizzata la pagina di aggiornamento delle transizioni di stato del ticket.

3. Selezionare le seguenti caselle di controllo in base alle specifiche esigenze:

   Consentito

   Specifica una transizione valida per lo stato. Utilizzare questa opzione per limitare i flussi di lavoro degli stati.

   Predefinito

   (Facoltativo) Specifica la transizione di stato predefinita. CA SDM applica la transizione predefinita quando gli utenti fanno clic sul pulsante della transizione predefinita nella pagina dei dettagli del ticket, oppure quando gli utenti (inclusi quelli del servizio Web) aggiornano la stato portandolo al valore <d>. È possibile configurare una sola transizione predefinita per ciascuno stato (o una per ciascun titolare in un sistema multi-tenancy).

   Commento necessario

   (Facoltativo) Specifica che un commento di registro attività per la transizione è richiesto in caso di modifica dello stato di un ticket.

   Nota: questa opzione è disponibile esclusivamente per i ticket di CA SDM. Non riguarda altre aree, ad esempio servizi Web o la funzionalità Modifica in elenco.

4. (Facoltativo) Selezionare un codice di stato nella colonna Nome per aggiornarne i dettagli.

5. Fare clic su Salva.

   Nell'elenco Transizioni viene visualizzato l'elenco delle transizioni configurate per il nuovo stato. Quando l'analista seleziona la casella a discesa Stato nella pagina dei ticket, viene visualizzato il nuovo elenco di stati.

Nota: per informazioni sulla procedura per definire transizioni di stato, consultare la *Guida in linea*.

Configurazione di controlli di attributo dipendenti

Con i controlli di attributo dipendenti è possibile stabilire quali campi vengono visualizzati o sono richiesti per lo stato del ticket.

Nota: prima di configurare attributi dipendenti come "richiesti" per un particolare stato, considerare che l'opzione Modifica in elenco che compare nella pagina di elenco del ticket potrebbe non visualizzare i valori di campi di attributo che sono richiesti. Se il valore del campo di attributo richiesto non fa già parte del ticket e se non è presentato nel formato Modifica in elenco, il ticket non viene salvato. Ne consegue che l'analista deve modificare i valori dei campi di attributo dipendenti nella pagina dei dettagli del ticket anzichè utilizzare l'opzione Modifica in elenco.

Per configurare un controllo di attributo dipendente

1. Nella pagina dei dettagli dello stato del ticket, selezionare la scheda Controllo attributo dipendente nella parte inferiore della pagina.

   Viene visualizzato l'Elenco controlli attributo.

2. Fare clic su Crea.

   Viene visualizzata la pagina Aggiorna controllo attributo dipendente.

3. Inserire i dati nei seguenti campi:

   Titolare

   (Facoltativo) In un sistema in cui è installata l'opzione multi-tenancy, specifica un nome titolare facoltativo. Se si specifica un titolare, la dipendenza si applica solo al titolare specificato e ai relativi titolari secondari.

   Attributo

   Specifica il nome dell'attributo da controllare, ad esempio, Riepilogo.

   Bloccato

   Specifica che l'attributo è bloccato. Non è possibile aggiornare un attributo bloccato associato a uno stato in un ticket con lo stesso stato. L'attributo viene sbloccato quando cambia lo stato.

   Richiesto

   Specifica che l'attributo è obbligatorio. Un attributo richiesto per lo stato non può utilizzare un valore nullo in un ticket con lo stesso stato.

4. Fare clic su Salva.

   Il nuovo controllo di attributo per lo stato viene visualizzato nell'Elenco controlli attributo quando la pagina viene nuovamente visualizzata. Quando un utente visualizza lo stato del ticket, il sistema recupera l'elenco degli attributi richiesti corrispondenti al nuovo stato e aggiorna la pagina del ticket in modo appropriato. Quando un utente tenta di chiudere il ticket senza compilare un campo richiesto, nella parte superiore della pagina del ticket viene visualizzato un messaggio di errore.

Nota: per informazioni sulla procedura per definire controlli di attributo dipendenti, consultare la *Guida in linea*.

Metodi dei servizi Web

È possibile configurare le transizioni di stato e i metodi dei servizi Web SOAP per il controllo dell'attributo dipendente seguenti:

getValidTransitions

Elenca le transizioni per un ticket. Questo metodo si basa sul metodo getValidTaskTransitions esistente, ad eccezione del fatto che l'argomento può essere un ticket o uno stato.

getDependentAttrControls

Elenca gli attributi bloccati e obbligatori per un attributo di un oggetto specificato dall'ID persistente. L'attributo Stato è supportato.

Nota: per ulteriori informazioni sui metodi dei servizi Web SOAP, consultare la *Guida di riferimento tecnico*.

Flussi di transizioni predefiniti

Per ogni tipo di ticket è possibile utilizzare transizioni di stato predefinite fornite con il prodotto e di modificarle in base al flusso di transizioni desiderato.

Nota: poiché è possibile condividere le transizioni di stato tra le integrazioni, ad esempio CA Workflow, non disattivare le transizioni di stato predefinite se non esplicitamente necessario.

Per visualizzare l'elenco delle transizioni predefinite, procedere come segue:

Nella scheda Amministrazione, espandere il nodo Service Desk e selezionare i seguenti elementi:

- Transizioni ordine di cambiamento
- Transizioni questione
- Transizioni richiesta/incidente/problema

Nell'elenco delle transizioni sono elencate le transizioni predefinite che consentono di controllare come un ticket (incidente/richiesta/problema, ordine di cambiamento e questione) proceda nel corso del proprio ciclo di vita.

Nota: per informazioni dettagliate su come definire e modificare le transizioni, vedere la *Guida in linea*.

Flusso delle transizioni degli incidenti

Nella tabella che segue viene riportato il flusso delle transizioni degli incidenti predefinito.

Stato corrente	Transizione predefinita	Stati successivi disponibili
Rilevato	In corso <d>	Evitato, In attesa del vendor, Annullato, Chiuso, Chiuso-Non risolto, In corso, Aperto, In attesa di cambiamento, Risolto
Evitato		Riconosciuto, Evitato, In attesa della risposta dell'utente finale, Chiuso, Chiuso-Non risolto, In corso, Rifiuta soluzione, Ricerca in corso, Risolto
In attesa della risposta dell'utente finale	Ricerca in corso <d>	Chiuso, Chiuso-Non risolto, In corso, Aperto, Ricerca in corso, Risolto
In attesa del vendor	Ricerca in corso <d>	Riconosciuto, Chiuso, Chiuso-Non risolto, In corso, Aperto, In attesa di cambiamento, Ricerca in corso, Risolto
Annullato		Chiuso

Stato corrente	Transizione predefinita	Stati successivi disponibili
Chiuso		Open (Aperto)
Chiuso-Non risolto		Rilevato
Chiuso-Non risolto		Chiuso
Chiuso-Non risolto		Open (Aperto)
In attesa		Riconosciuta, Chiuso, In corso, Aperto, In attesa di cambiamento, Risolto
In corso	Ricerca in corso <d>	Riconosciuta, In attesa della risposta dell'utente finale, In attesa del vendor, Chiuso, Chiuso-Non risolto, Aperto, In attesa di cambiamento, Ricerca in corso, Risolto
Pending Change (Modifica in sospeso)	Ricerca in corso <d>	Riconosciuto, Chiuso, In corso, Aperto, Risolto
Researching	Risolto <d>	Chiuso, Aperto, Risolto
Risolto	Chiuso <d>	In attesa della risposta dell'utente finale, Chiuso, Aperto

Flusso delle transizioni dei problemi

Nella tabella che segue viene riportato il flusso delle transizioni dei problemi predefinito.

Stato corrente	Transizione predefinita	Stati successivi disponibili
Rilevato	In corso <d>	Riconosciuto, Approvato, Annullato, Chiuso, Correzione in corso, Aperto, Respinto, Ricerca in corso
Analisi completata	Approvato <d>	Riconosciuto, Annullato, Chiuso, Correzione in corso
Approvato	Correzione in corso <d>	Chiuso, Corretto, In attesa di cambiamento
In attesa del vendor	Ricerca in corso <d>	Riconosciuto, Chiuso, Chiuso-Non risolto, Corretto, In corso, Aperto, In attesa di cambiamento, Ricerca in corso
Annullato	Chiuso <d>	Chiuso, Chiuso-Non risolto, Aperto
Chiuso-Non risolto		Riconosciuta, Chiuso, Aperto
Correzione in corso	Corretto <d>	Approvato, Annullato, Corretto, Correzione in corso, Ricerca in corso, Respinto
Fisso	Chiuso <d>	Chiuso

Stato corrente	Transizione predefinita	Stati successivi disponibili
In attesa	Ricerca in corso <d>	Riconosciuto, Chiuso, Corretto, In corso, Aperto, In attesa di cambiamento, Ricerca in corso
In corso	Ricerca in corso <d>	Riconosciuto, Approvato, Annullato, Chiuso, Correzione in corso, In attesa di cambiamento, Respinto, Ricerca in corso
Errore noto	Correzione in corso <d>	Chiuso, Correzione in corso, Corretto
Open (Aperto)	Riconosciuta <d>	Riconosciuto, Approvato, Annullato, Chiuso, Correzione in corso, In corso, Respinto, Ricerca in corso
Pending Change (Modifica in sospeso)	Corretto <d>	Chiuso, Corretto, Ricerca in corso
Rifiutato	Chiuso <d>	Chiuso, Chiuso-Non risolto, Aperto
Researching	Analisi completata <d>	Riconosciuto, Analisi completata, Approvato, Annullato, Chiuso, Correzione in corso, Corretto, Respinto

Flusso delle transizioni delle questioni

Nella tabella che segue viene riportato il flusso delle transizioni delle questioni predefinito.

Stato corrente	Transizione predefinita	Stati successivi disponibili
Rilevato	In corso <d>	In attesa della risposta dell'utente finale, In attesa del vendor, Chiuso, Chiuso-Non risolto, In corso, Aperto, In attesa di cambiamento, Risolto
In attesa della risposta dell'utente finale	Ricerca in corso <d>	Riconosciuto, Chiuso, Chiuso-Non risolto, In corso, Aperto, Ricerca in corso, Risolto
In attesa del vendor	Ricerca in corso <d>	Riconosciuto, Chiuso, In corso, Aperto, In attesa di cambiamento, Ricerca in corso, Risolto
Annullato	Chiuso <d>	Chiuso
Chiuso		Riconosciuto, Aperto
Chiuso-Non risolto		Riconosciuta, Chiuso, Aperto
In attesa		Riconosciuta, Chiuso, In corso, Aperto, In attesa di cambiamento, Risolto

Stato corrente	Transizione predefinita	Stati successivi disponibili
In corso	Ricerca in corso <d>	Riconosciuta, In attesa della risposta dell'utente finale, In attesa del vendor, Chiuso, Chiuso-Non risolto, Aperto, In attesa di cambiamento, Ricerca in corso, Risolto
Open (Aperto)	Riconosciuta <d>	Riconosciuto, Evitato da Self-Service, In attesa della risposta dell'utente finale, In attesa del vendor, Chiuso, Chiuso-Non risolto, In corso, In attesa di cambiamento, Risolto
Pending Change (Modifica in sospeso)	Ricerca in corso <d>	Riconosciuto, Chiuso, In corso, Aperto, Ricerca in corso, Risolto
Researching	Risolto <d>	Chiuso, Aperto, Risolto, In attesa della risposta dell'utente finale, Chiuso, Aperto

Flusso delle transizioni degli ordini di cambiamento

Nella tabella che segue viene riportato il flusso delle transizioni degli ordini di cambiamento predefinito.

Stato corrente	Transizione predefinita	Stati successivi disponibili
Approvazione in corso	Approvato <d>	Approvato, Annullato, Chiuso
Approvato	Pianificato <d>	Annullato, Chiuso, Implementazione in corso, Pianificato
Ritirato		Approvazione in corso, Chiuso, Aperto, RFC
Annullato		Chiuso
Sospensione cliente		Annullato, Chiuso, Implementazione in corso, Respinto, Pianificato, Verifica in corso
In attesa		Annullato, Chiuso, Implementazione in corso, Pianificato
Implementazione in corso		Ritirato, Annullato, Chiuso, Sospensione cliente, Respinto, Pianificato, Sospensione vendor, Verifica in corso
Open (Aperto)	RFC <d>	Approvazione in corso, Annullato, Chiuso, Sospensione cliente, Implementazione in corso, Respinto, RFC, Pianificato, Sospensione vendor
Rifiutato	Chiuso <d>	Approvazione in corso, Annullato, Chiuso
RFC	Approvazione in corso <d>	Approvazione in corso, Annullato, Chiuso, Sospensione cliente, Implementazione in corso, Aperto, Respinto, Pianificato, Sospensione vendor

Stato corrente	Transizione predefinita	Stati successivi disponibili
Pianificato	Implementazione in corso <d>	Annullato, Chiuso, Sospensione cliente, Implementazione in corso, Sospensione vendor, Verifica in corso, Annullato, Chiuso, Implementazione in corso, Pianificato, Ritirato, Chiuso

Procedura ottimale: Transizioni di stato predefinite

Le transizioni di stato fornite con il prodotto sono attive nella nuova installazione e disattivate in seguito all'aggiornamento. Per ciascun stato elencato nella pagina Elenco Transizioni, è presente una transizione stato predefinita (o uno stato successivo). Il percorso assunto dalla transizione stato predefinita corrisponde alla procedura ottimale. Le transizioni stato di aggiuntive presenti nella pagina Elenco transizioni vengono fornite per soddisfare i diversi flussi di lavoro di gestione dei ticket. Tuttavia, solo le transizioni di stato attive che usano questa procedura ottimale garantiscono l'esecuzione del flusso di lavoro corretto per la gestione di Richieste, Incidenti, Problemi e Ordini di cambiamento. La procedura ottimale aiuta a promuovere lo spostamento dei ticket verso la risoluzione e la chiusura nell'ambiente IT.

Ad esempio, le seguenti transizioni Incidente predefinite presenti nella pagina Elenco Transizioni Incidente sono impostate su Non attivo per consentire la risoluzione e la chiusura degli incidenti:

Stato	Nuovo stato	Predefinito	status_description	Stato record
Accettato	Chiuso	No	Transizione di stato: da Accettato a Chiuso	Non attivo
Accettato	Chiuso-Non risolto	No	Transizione di stato: da Accettato a Chiuso - Non risolto	Non attivo
Accettato	Aperto	Sì	Transizione di stato: da Accettato ad Aperto	Non attivo
In attesa della risposta dell'utente finale	Accettato	No	Transizione di stato: da In attesa della risposta dell'utente finale a Accettato	Non attivo
In attesa della risposta dell'utente finale	Aperto	No	Transizione di stato: da In attesa della risposta dell'utente finale a Aperto	Non attivo
In attesa del vendor	Accettato	No	Transizione di stato: da In attesa del vendor a Accettato	Non attivo

Stato	Nuovo stato	Predefinito	status_description	Stato record
In attesa del vendor	Chiuso	No	Transizione di stato: da In attesa del vendor a Chiuso	Non attivo
In attesa del vendor	Aperto	No	Transizione di stato: da In attesa del vendor ad Aperto	Non attivo
Chiuso	Accettato	No	Transizione di stato: da Chiuso a Accettato	Non attivo
Chiuso-Non risolto	Accettato	No	Transizione di stato: da Chiuso - Non risolto a Accettato	Non attivo
Chiuso-Non risolto	Chiuso	No	Transizione di stato: da Chiuso - Non risolto a Chiuso	Non attivo
In attesa	Accettato	No	Transizione di stato: da In attesa a Accettato	Non attivo
In attesa	Chiuso	No	Transizione di stato: da In attesa a Chiuso	Non attivo
In attesa	Aperto	No	Transizione di stato: da In attesa ad Aperto	Non attivo
In corso	Accettato	No	Transizione di stato: da In corso a Accettato	Non attivo
In corso	Chiuso	No	Transizione di stato: da In corso a Chiuso	Non attivo
In corso	Aperto	No	Transizione di stato: da In corso ad Aperto	Non attivo
Aperto	Chiuso	No	Transizione di stato: da Aperto a Chiuso	Non attivo
In attesa di Cambiamento	Accettato	No	Transizione di stato: da In attesa di cambiamento a Accettato	Non attivo
In attesa di Cambiamento	Chiuso	No	Transizione stato: da In attesa di Cambiamento a Chiuso	Non attivo
In attesa di Cambiamento	Aperto	No	Transizione stato: da In attesa di Cambiamento ad Aperto	Non attivo
Ricerca	Aperto	No	Transizione di stato: da Ricerca a Aperto	Non attivo

Transizioni di stato per l'interfaccia self-service

Le transizioni di stato consentono di controllare il movimento di un ticket da uno stato discreto all'altro (ad esempio da Aperto a Chiuso). Per i dipendenti che utilizzano l'interfaccia self-service, è possibile includere nei moduli Dettagli Incidente e Dettagli Richiesta dei pulsanti che rappresentino le transizioni di stato (a pagina 437).

I pulsanti delle transizioni di stato per i flussi di lavoro di elaborazione di Incidenti e Problemi vengono visualizzati nell'interfaccia del dipendente se le transizioni di Incidenti e RIchieste sono collegati a tipi di transizione attivi. Un tipo di transizione definisce il testo del pulsante e controlla il comportamento del modulo dei dettagli del ticket. Quando vengono definiti i pulsanti, i pulsanti legacy Chiudi Incidente (o Richiesta) e Riapri Incidente (o Richiesta) non vengono visualizzati nei moduli dei dettagli del ticket. Il dipendente potrà solo modificare lo stato dell'incidente o della richiesta utilizzando i pulsanti di transizione di stato configurati dall'amministratore.

Per impostazione predefinita, tutti i tipi di transizione predefiniti forniti con il prodotto non sono attivi, pertanto i pulsanti di transizione di stato non sono abilitati. L'amministratore di sistema può attivare e modificare i tipi di transizione predefiniti oppure creare tipi di transizione che soddisfino il flusso delle transizioni di stato in uso nell'organizzazione. Dopo aver creato o modificato un tipo di transizione, è possibile collegarlo a una qualsiasi transizione di stato di Incidente o Richiesta.

Nota: per ulteriori informazioni sull'uso dei tipi di transizione, consultare la *Guida in linea*.

Ulteriori informazioni:

Modalità di funzionamento delle transizioni per l'interfaccia self-service (a pagina 448)
Modalità di creazione o aggiornamento di tipi di transizione per le transizioni (a pagina 449)
Modalità di collegamento dei tipi di transizione alle transizioni (a pagina 450)
Attivazione dei tipi di transizione predefiniti (a pagina 450)

Modalità di funzionamento delle transizioni per l'interfaccia self-service

I tipi di transizione e i controlli degli stati corrispondenti controllano la modalità con cui i dipendenti possono aprire e riaprire ticket nel modo illustrato di seguito:

1. Tipi di transizione attivi vengono collegati a transizioni di stato di incidenti (o richieste) dall'amministratore.
2. Il dipendente crea un incidente utilizzando l'interfaccia self-service.
3. L'analista assegnato all'incidente trova una soluzione e imposta il ticket sullo stato Risolto.

4. Quando lo stato di un ticket è Risolto, nel modulo dei dettagli del dipendente vengono visualizzati i pulsanti di transizione di stato per accettare o rifiutare la risoluzione.
   - Se il dipendente accetta la risoluzione, viene eseguita la transizione da Risolto a Chiuso.
   - Se il dipendente rifiuta la risoluzione, viene eseguita la transizione da Risolto ad Aperto
5. Dopo che il dipendente ha fatto clic su un pulsante, aggiunge i propri commenti nel modulo visualizzato.

Modalità di creazione o aggiornamento di tipi di transizione per le transizioni

L'amministratore di sistema può creare nuovi tipi di transizione o aggiornare quelli esistenti per fluissi di lavoro di transizioni di stato di richieste e incidenti nella pagina Elenco tipi di transizione.

Per creare un tipo di transizione per una transizione di stato, procedere come segue:

1. Nella scheda Amministrazione, selezionare Service Desk, Richieste/Incidenti/Problemi, Tipi di transizione.
2. Fare clic su Crea nella pagina dell'elenco.
3. Modificare i campi secondo necessità nella pagina dei dettagli.

   Il tipo di transizione per la transizione di stato viene creato.
4. Fare clic su Salva.

   Il nuovo tipo di transizione vene visualizzato nella pagina Elenco tipi di transizione quando quest'ultima viene rivisualizzata.

Per attivare un tipo di transizione predefinito, procedere come segue:

1. Aprire il tipo di transizione desiderato per modificarlo nella pagina Elenco Tipi di transizione.
2. Modificare i campi in modo appropriato.
3. Fare clic su Salva.

   Il tipo di transizione aggiornato compare nell'elenco Tipo di transizione.

Modalità di collegamento dei tipi di transizione alle transizioni

Quando le transizioni di stato sono collegate ai tipi di transizione, nel modulo dei dettagli ticket del dipendente vengono visualizzati i pulsanti di transizione per accettare o rifiutare la risoluzione. Per collegare un tipo di transizione a una transizione di stato, procedere come segue:

1. Nella scheda Amministrazione, selezionare Service Desk, Richieste/Incidenti/Problemi, Transizioni incidente (o richiesta).
2. Aprire la transizione di stato desiderata per modificarla nella pagina Elenco transizioni richiesta o Elenco transizioni incidente.
3. Specificare il tipo di transizione desiderato nel campo Tipo di transizione.
4. Fare clic su Salva.

   Il tipo di transizione è collegato alla transizione di stato.

Attivazione dei tipi di transizione predefiniti

Per impostazione predefinita, tutti i tipi di transizione predefiniti forniti con il prodotto non sono attivi, pertanto i pulsanti di transizione di stato non sono abilitati. È possibile attivare e modificare questi tipi di transizione in base alle proprie esigenze in termini di flusso di transizioni di stato.

Attivazione di un tipo di transizione predefinito

1. Selezionare Mostra filtro nella pagina Elenco Tipi di transizione.

   Nella parte superiore della pagina sono visualizzati i campi di ricerca aggiuntivi.
2. Nel campo Stato record, selezionare Non attivo e fare clic su Cerca.

   L'elenco Tipi di transizione visualizza tutti i tipi di transizione non attivi.
3. Fare clic con il pulsante destro del mouse sul tipo di transizione desiderato e selezionare Modifica dal menu di scelta rapida.
4. Selezionare Attivo nel campo Stato record.
5. Fare clic su Salva, quindi su Chiudi finestra.
6. Fare clic su Cerca.

   L'elenco Tipi di transizione mostra il tipo di transizione attivo.

Ulteriori informazioni:

Tipi di transizione predefiniti per le transizioni di stato dell'Incidente (a pagina 451)
Tipi di transizione predefiniti per le transizioni di stato della Richiesta (a pagina 451)

Tipi di transizione predefiniti per le transizioni di stato dell'Incidente

La tabella seguente descrive i tipi di transizione predefiniti per le transizioni di stato degli Incidenti:

Simbolo	Testo del pulsante	Intestazione del modulo	Transizione di stato dell'Incidente
Pulsante Accetta risoluzione incidente	Accetta	Accetta risoluzione	da Risolto a Chiuso
Pulsante Rifiuta risoluzione incidente	Rifiuta	Rifiuta risoluzione	da Risolto a Aperto
Pulsante Richiedi chiusura Incidente	Richiedi chiusura	Richiedi chiusura	■ da Chiuso - Non risolto ad Aperto ■ In attesa della risposta dell'utente finale ■ In attesa del vendor ■ In corso ■ Accettato

Tipi di transizione predefiniti per le transizioni di stato della Richiesta

La tabella seguente descrive i tipi di transizione predefiniti per le transizioni di stato della Richiesta:

Nota: lo stato Chiusura richiesta delle Richieste equivale allo stato Risolto degli Incidenti.

Simbolo	Testo del pulsante	Intestazione del modulo	Transizione di stato della Richiesta
Pulsante Accetta risoluzione richiesta	Accetta	Accetta risoluzione	da Chiusura richiesta a Chiuso
Pulsante Rifiuta risoluzione richiesta	Rifiuta	Rifiuta risoluzione	da Chiusura richiesta a Aperto
Pulsante Richiedi chiusura richiesta	Richiedi chiusura	Richiedi chiusura	■ da Aperto ad Annullato ■ In attesa della risposta dell'utente finale ■ In attesa del vendor ■ Approvazione in corso ■ Accettato

Simbolo	Testo del pulsante	Intestazione del modulo	Transizione di stato della Richiesta
Pulsante Chiudi richiesta	Chiusura	Chiusura richiesta	Da In corso a Chiuso

Timer

I timer agiscono come un cronometro con varie soglie che forniscono agli analisti indicazioni sul tempo trascorso. È possibile definire un periodo di tempo per ogni soglia e, quando questa soglia viene raggiunta, impostare il timer affinché cambi colore, emetta un segnale acustico o visualizzi un promemoria. Un analista del service desk non può controllare il timer, solo l'amministratore può controllarlo.

Le richieste rappresentano l'unico tipo di ticket che utilizza i timer; quindi, occorre impostare i timer per i modelli di service desk interni e combinati.

Di seguito sono riportati i valori di soglia predefiniti per il timer:

Durata limite	Colore
00:00:00	Verde
00:01:00	Giallo
00:05:00	Rosso

In base ai valori predefiniti, all'avvio il timer è di colore verde. Dopo un minuto, il timer diventa di colore giallo. Dopo cinque minuti, diventa di colore rosso. Il tempo trascorso viene mostrato quando l'analista visualizza la richiesta in dettaglio e viene azzerato quando viene selezionata una nuova richiesta. A questo processo è possibile aggiungere delle fasi o modificare le fasi esistenti.

Il timer può essere contrassegnato come attivo o non attivo. Quando si contrassegna il timer come non attivo, non fa più parte del processo ma resta disponibile per un utilizzo futuro, in quanto non viene eliminato dal database. Se in seguito si decide di utilizzare il timer, contrassegnarlo come attivo.

Fusi orari

Nel sistema CA SDM è possibile impostare fusi orari specifici per server, tipi di servizi, contatti e posizioni. È possibile configurare tipi di servizi locali validi per un fuso orario specifico e tipi di servizi globali validi in tutta l'organizzazione. Grazie a questa configurazione, l'amministratore non sarà più obbligato a conoscere il fuso orario di un server e a regolare manualmente gli orari dei turni in modo che si adattino ai vari fusi orari.

Ulteriori informazioni:

Attivazione di eventi tipo di servizio (a pagina 453)
Evento attivato dal fuso orario (a pagina 454)
Regole fuso orario (a pagina 454)

Attivazione di eventi tipo di servizio

I tipi di servizio definiscono gli eventi attivati dopo un ritardo specificato.

Esempio: attivazione di eventi per pianificazione dei turni

In questo esempio, una pianificazione dei turni associata al tipo di servizio vincola l'ora effettiva in cui viene attivato un evento, come descritto di seguito:

- Il turno di lavoro è dalle 8:00 alle 17:00
- Il ritardo dell'evento è tre ore
- L'ora corrente del server corrisponde alle 15:00

L'evento viene attivato domani alle 9:00 ora del server perché:

- Secondo l'ora attuale del server rimangono due ore nel turno di lavoro odierno (ora sono le 15.00. Il turno termina alle 17.00).
- Il ritardo dell'evento è tre ore. Due ore di questo ritardo vengono spese nel turno di lavoro odierno (dalle 15:00 alle 17:00). Un'ora di ritardo aggiuntiva viene trasferita al turno di lavoro del giorno successivo (dalle 08:00 alle 9:00).

Di conseguenza l'evento inizia elle 9:00 del giorno successivo.

Evento attivato dal fuso orario

L'ora di attivazione di un evento può essere vincolata da un fuso orario associato al tipo di servizio.

Esempio: Evento attivato dal fuso orario

In questo esempio, un fuso orario associato al tipo di servizio vincola l'ora effettiva in cui viene attivato un evento, come descritto di seguito:

- Il turno di lavoro è dalle 8:00 alle 17:00
- Il ritardo dell'evento è tre ore
- L'ora corrente del server corrisponde alle 15:00
- L'ora corrente del fuso orario corrisponde alle 12:00

L'evento viene attivato oggi alle 18:00 ora del server perché:

- Secondo l'ora attuale del server rimangono due ore nel turno di lavoro odierno (ora sono le 15.00. Il turno termina alle 17.00).
- Secondo l'ora attuale del fuso orario rimangono cinque ore nel turno di lavoro di oggi (ora sono le 12.00. Il turno termina alle 17.00).
- Il ritardo dell'evento è di tre ore (dalle 00:00 alle 15:00 ora del fuso orario. e dalle 15:00 alle 18:00 ora del server).

Pertanto l'evento inizia alle 18:00 ora del server o alle 15:00 ora del fuso orario.

Regole fuso orario

È possibile specificare un fuso orario per un server, per una posizione o per un tipo di servizio. È inoltre possibile richiedere a CA SDM di utilizzare il fuso orario dell'Utente finale interessato da un ticket. CA SDM utilizza le regole seguenti per determinare quale fuso orario attiva un evento:

- **Fuso orario dell'utente finale interessato**—CA SDM utilizza questa regola se esistono le seguenti condizioni:
  - È selezionata l'opzione Utilizza fuso orario dell'utente finale.
  - È specificato un fuso orario per l'utente finale interessato del ticket.
- **Fuso orario della posizione dell'utente finale interessato**—CA SDM utilizza questa regola se esistono le seguenti condizioni:
  - È selezionata l'opzione Utilizza fuso orario dell'utente finale.
  - Non è specificato un fuso orario per l'utente finale interessato del ticket.
  - È specificato un fuso orario per la posizione dell'utente finale interessato.

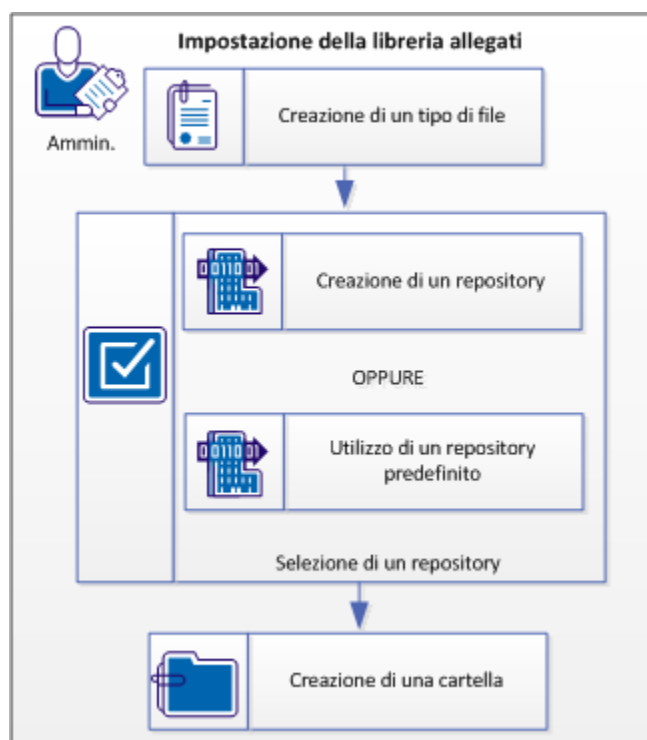
- **Fuso orario del tipo di servizio**—CA SDM utilizza questa regola se esistono le seguenti condizioni:
  - È specificato un fuso orario per il tipo di servizio.
  - Non è selezionata l'opzione Utilizza fuso orario dell'utente finale.
- **Fuso orario del server**—CA SDM utilizza questa regola se esistono le seguenti condizioni:
  - È specificato un fuso orario per il server.
  - Non è selezionata l'opzione Utilizza fuso orario dell'utente finale.
  - Non è specificato un fuso orario per il tipo di servizio.
- **Fuso orario non supportato**—CA SDM utilizza questa regola se esistono le seguenti condizioni:
  - Non è specificato un fuso orario per il tipo di servizio.
  - Non è selezionata l'opzione Utilizza fuso orario dell'utente finale.
  - Non esistono record del server.

Modalità di configurazione della libreria allegati

È possibile aggiungere tipi diversi di allegati alle varie entità di CA SDM. Ad esempio, un cliente può associare la snapshot di un errore all'incidente. L'utente amministratore configura la libreria degli allegati dalla quale gli utenti possono caricare o scaricare allegati.

È possibile classificare gli allegati nel modo seguente:

- **Archiviato**: il server Web utilizza il protocollo HTTP per caricare e memorizzare gli allegati archiviati in un repository. Quando un analista esamina un allegato archiviato, il file viene recuperato dal repository e visualizzato localmente. L'utilizzo di un server Web per la memorizzazione dei file consente l'archiviazione e il recupero dall'interfaccia utente.
- **Collegato**: nel database viene memorizzato solo un collegamento al file.

Il diagramma seguente mostra come configurare una libreria di allegati:

Procedere come descritto di seguito:

1. Aprire l'interfaccia utente Web di CA SDM. (a pagina 191)
2. Creare un tipo di file. (a pagina 457)
3. Scegliere il repository (a pagina 458).
   - Configurare un repository su un computer remoto (a pagina 459).
   - Creare un repository (a pagina 460).
   - Utilizzare un repository predefinito (a pagina 460).
4. Creare una cartella (a pagina 464).

Apertura dell'interfaccia utente Web di CA SDM

Accedere all'interfaccia utente Web dai server seguenti, in base alla configurazione di CA SDM:

- Convenzionale: server primario o secondario
- Disponibilità avanzata: server applicazioni o in background

Creazione di un tipo di file

CA SDM fornisce tipi di file predefiniti che possono supportare gli allegati. Ad esempio, il tipo di file predefinito Adobe Acrobat supporta i formati file di pdf come allegati. È inoltre possibile creare nuovi tipi di file. Ad esempio, creare tipo di file JPEG perché gli utenti possano caricare le snapshot degli incidenti.

Procedere come descritto di seguito:

1. Accedere all'interfaccia utente Web dai seguenti server di CA SDM, a seconda della configurazione di CA SDM:
   - Convenzionale: server primario o secondario
   - Disponibilità avanzata: server applicazioni o in background
2. Selezionare Libreria allegati, Tipi di file nella scheda Amministrazione.

   Viene visualizzata la pagina Elenco Tipi di file.
3. Fare clic su Crea Nuovo.

   Viene visualizzata la pagina Crea Nuovo tipo di file.
4. Inserire i dati nei seguenti campi:

   Tipo

   Specifica il tipo di file o identifica l'applicazione software associata, ad esempio un documento Word, un'immagine o un file eseguibile.

   Estensione

   Specifica i caratteri aggiunti al nome file di base che identificano il tipo di file. Ad esempio, l'estensione doc identifica un documento Microsoft Word.

   Nome icona

   Specifica il nome del file grafico che contiene l'icona utilizzata per identificare il tipo di file.

   Stato

   Indica se il record è attivo nel database e disponibile per l'utilizzo.
5. Fare clic su Salva.

   Il tipo di file viene creato.

Scelta del repository

Gli allegati vengono archiviati in repository ed è necessario configurare i repository prima che gli utenti possano lavorare con gli allegati. È possibile aggiungere quanti repository si desiderano per rispondere al meglio alle esigenze della propria organizzazione. Ad esempio, è possibile aggiungere repository separati per memorizzare le immagini e i file allegati. Inoltre, è possibile aggiungere le cartelle ai repository per organizzare ulteriormente i file, quindi caricarli nelle posizioni corrette.

Tutte le interfacce client possono accedere ai repository esistenti per caricare e scaricare gli allegati di file, tranne che nei seguenti casi:

- I repository di file condivisi sono accessibili solo se il daemon dei repository è in esecuzione su un computer in grado di accedere ai file condivisi. Il nome server nel record repository (modulo dei dettagli) deve corrispondere a un computer Windows che ha accesso ai file condivisi. È necessario che su tale computer sia in esecuzione anche un daemon del repository di CA SDM.
- Il download dei file zip dipende da quando sono stati caricati. Gli allegati creati in versioni precedenti vengono scaricati senza eseguirne la decompressione. Decomprimere il file sul computer client. Altrimenti, gli allegati caricati da un'interfaccia client vengono anche scaricati senza essere decompressi. Quindi, il server decomprime il file prima di restituirlo, durante una richiesta di download del client.

L'architettura distribuita consente a un sito di configurare i propri repository secondo le esigenze del caso. Il servlet di un repository non deve trovarsi sullo stesso server dei file allegati. È possibile scegliere per i siti un servlet centrale per l'accesso ai repository distribuiti oppure un servlet dedicato per ognuno dei server di repository.

Prendere in considerazione le seguenti configurazioni dei repository:

- **Server di repository su un server di CA SDM protetto**—I siti che specificano un server di repository su un server di CA SDM protetto da firewall non devono necessariamente esporre il servlet su tale computer. Possono piuttosto specificare un servlet in esecuzione su un altro server di CA SDM o su un server di CA SDM senza limitazioni ed eseguire operazioni di caricamento e download su tale repository. A seconda della rete tra il server repository e il server servlet, può verificarsi qualche impatto sulle prestazioni durante il caricamento e il download. Un metodo valido per configurare un repository remoto è quello di installare e configurare un altro server insieme al repository sul server remoto e impostare il percorso di caricamento su un percorso locale. Per ulteriori informazioni, consultare l'argomento Configurazione di un repository su un computer remoto (a pagina 459).
- **Servlet sullo stesso server del server del repository** - Questa configurazione è ideale per i siti che desiderano prestazioni ottimali per il caricamento e il download degli allegati, nel caso in cui le prestazioni della rete siano di importanza fondamentale e se vengono allegati file di grandi dimensioni. Questo tipo di approccio richiede l'utilizzo della porta Tomcat (solitamente la 8080) sul server e dovrebbe essere preso in considerazione se il computer è protetto da un firewall.

CA SDM fornisce repository predefiniti e consente anche di creare i propri repository per rispondere al meglio alle esigenze della propria organizzazione. Scegliere una delle seguenti opzioni:

- Creare un repository (a pagina 460).
- Utilizzare un repository predefinito (a pagina 460).

Configurazione di un repository su un computer remoto

Per impostazione predefinita, i repository si trovano sul server seguente, a seconda della configurazione di CA SDM:

- Convenzionale: server primario
- Disponibilità avanzata: server in background

I repository predefiniti utilizzano sia il servlet sia il daemon del repository (rep_daemon) di questi server. Per creare un repository su un computer remoto è necessario installare e configurare i server seguenti, a seconda della configurazione di CA SDM:

- Convenzionale: server secondario. Il servlet viene eseguito sul server primario e il daemon rep_daemon viene eseguito sul server secondario.
- Disponibilità avanzata: server in background. Il servlet viene eseguito sul server applicazioni e il daemon rep_daemon viene eseguito sul server in background.

Nella configurazione di disponibilità avanzata, il daemon rep_daemon viene eseguito su tutti i server per impostazione predefinita.

Nella configurazione convenzionale, il daemon rep_daemon viene eseguito sul server primario per impostazione predefinita ed è necessario verificare che il daemon rep_daemon sia eseguito sul server secondario per questa configurazione.

(Solo configurazione convenzionale) Procedere come descritto di seguito:

1. Selezionare Sistema, Configurazioni nella scheda Amministrazione.

   Viene visualizzata la pagina Elenco configurazioni.
2. Selezionare la configurazione per il server secondario.

   Viene visualizzata la pagina Dettagli configurazione.
3. Fare clic su Processi aggiuntivi.

   Viene visualizzato l'elenco dei processi aggiuntivi.
4. Fare clic su Aggiungi processo.
5. Selezionare il daemon del repository come processo.
6. Fare clic su Salva.

   Il repository viene installato sul server secondario.

Creazione di un repository allegati

A seconda delle proprie esigenze di organizzazione, è possibile avere un repository di grandi dimensioni o più repository di piccole dimensioni. Lo spostamento o la combinazione dei repository avviene facilmente in quanto tutti gli attributi di un repository vengono definiti nel relativo record.

Procedere come descritto di seguito:

1. Selezionare Libreria allegati, Repository nella scheda Amministrazione.

   Viene visualizzata la pagina Repository.

2. Fare clic su Crea Nuovo.

   Viene visualizzata la pagina Crea Nuovo repository.

   Nota: Per il fornitore del servizio è necessario selezionare il titolare appropriato nella pagina Crea Nuovo repository. L'opzione pubblica (condivisa) rende il repository disponibile per tutti i titolari.

3. Compilare i campi relativi al repository in modo appropriato.
4. Fare clic su Salva.

   Il repository è stato creato.

Utilizzo di un repository allegati predefinito

È possibile utilizzare un repository predefinito (Service Desk o Conoscenza o Immagini). È possibile modificare un repository per rispondere al meglio alle esigenze dell'organizzazione.

Procedere come descritto di seguito:

1. Selezionare Libreria allegati, Repository nella scheda Amministrazione.

   Viene visualizzata la pagina Elenco repository.

2. Fare clic con il pulsante destro del mouse sul repository che si desidera modificare e selezionare Modifica.

   Viene visualizzata la pagina Aggiorna repository.

3. Modificare i campi in modo appropriato. Per ulteriori informazioni, consultare l'argomento Campi del repository.
4. Fare clic su Salva.

   La definizione del repository viene salvata.

Campi Repository

I campi seguenti vengono utilizzati per modificare o creare un repository.

Nome

Specifica il nome per identificare il repository in modo univoco. Ad esempio, nel repository Immagini incidente è possibile archiviare tutte le immagini correlate a un incidente.

Tipo repository

Indica il tipo di contenuto archiviato nel repository. Ad esempio, per archiviare allegati di immagine, selezionare Immagini.

Valore predefinito

Indica se è il repository predefinito per il tipo di repository specificato. Ad esempio, quando l'utente crea un incidente e desidera associarvi un allegato, viene visualizzato il repository predefinito per la selezione. È possibile impostare come predefinito solo un repository.

Dimensione limite file (KB)

Specifica la dimensione massima di file, in kilobyte, che è possibile caricare nel repository.

Percorso caricamento

Specifica il percorso completo della directory principale o il percorso UNC in cui si trovano i file caricati nel repository.

Credenziali UNC

Specifica le credenziali per accedere al percorso UNC specificato nel campo Percorso di caricamento. Fare clic su Credenziali UNC per aprire la pagina Ricerca credenziali.

- Se sono state già create le credenziali per accedere al percorso UNC specificato, usare i campi per cercare e selezionare le credenziali.
- Se si desidera creare le credenziali, fare clic su Crea Nuovo. Per ulteriori informazioni sulla creazione di credenziali, consultare l'argomento Creazione di credenziali UNC (a pagina 463).

Servizi in background

Specifica i servizi del server in background per il percorso di servlet e rep_daemon.

Nessuno

Indica che il server in background non viene utilizzato per il percorso di servlet o per rep_daemon. Se si seleziona questa opzione, immettere i valori nei campi Server servlet e Server repository.

Solo servlet

Indica che il servlet è ospitato sul server in background. Se si seleziona questa opzione, il campo Server servlet viene compilato in modo automatico con il valore di Server in background. Immettere il valore per il campo Server repository. Se il server in background si arresta e il server di standby viene promosso a nuovo server in background, il campo Server servlet viene compilato con il valore del nuovo server in background.

Solo Daemon

Indica che rep_daemon viene eseguito sul server in background. Se si seleziona questa opzione, il campo Server repository viene compilato in modo automatico con il valore di Server in background. Immettere il valore per il campo Server servlet. Se il server in background si arresta e il server di standby viene promosso a nuovo server in background, il campo Server repository viene compilato con il valore del nuovo server in background.

Servlet e daemon

Indica che il server in background viene utilizzato per il percorso di servlet e per rep_daemon. Se si seleziona questa opzione, i campi Server servlet e Server repository vengono compilati in modo automatico con il valore di Server in background. Se il server in background si arresta e il server di standby viene promosso a nuovo server in background, questi campi vengono compilati con il valore del nuovo server in background.

Server servlet

Specifica il server di esecuzione del servlet.

Server repository

Specifica il server su cui rep_daemon è attivo e in esecuzione.

Tipo archivio

Specifica l'azione di archiviazione ed eliminazione da eseguire sul contenuto del repository.

Nessuno

Non vengono eseguiti processi di archiviazione ed eliminazione.

Archiviazione ed eliminazione

I record della cronologia vengono scritti nel file specificato nel campo di archiviazione ed eliminati dal database.

Elimina solamente

I record della cronologia vengono eliminati dal database, senza essere scritti nel file di archiviazione.

Percorso archivio

Specifica il percorso della directory o il percorso UNC in cui vengono spostati i file nel repository durante il processo di archiviazione.

Credenziali UNC

Specifica le credenziali per accedere al percorso UNC. Fare clic su Credenziali UNC per aprire la pagina Ricerca credenziali.

- Se sono state già create le credenziali per accedere al percorso UNC specificato, usare i campi per cercare e selezionare le credenziali.
- Se si desidera creare le credenziali, fare clic su Crea Nuovo. Per ulteriori informazioni sulla creazione di credenziali, consultare l'argomento Creazione di credenziali UNC (a pagina 463).

Tipi file proibiti

Indica l'estensione dei file che non è possibile caricare nel repository.

Nota: se il valore in questo campo inizia con un punto esclamativo (!), si tratta di tipi di file consentiti nel repository corrente. Ad esempio, jpg,gif all'interno dell'elenco indica che i file .jpg e .gif sono proibiti nel repository. Tuttavia, un valore !jpg,gif indica che solo i file con estensione .jpg e .gif sono ammessi nel repository.

Creazione delle credenziali UNC

Le credenziali UNC si creano per consentire agli utenti di accedere alle risorse condivise dai server di CA SDM mediante il percorso UNC.

Importante. Il componente UNC non funziona quando il server CA SDM si trova nel dominio e la posizione condivisa è nel GRUPPO DI LAVORO. Non funziona nemmeno quando la password dell'amministratore per il server CA SDM e la posizione condivisa sono diversi.

Procedere come descritto di seguito:

1. Fare clic su Credenziali UNC nella pagina Impostazioni generali o selezionare Gestione protezione e ruoli, Credenziali UNC nella scheda Amministrazione.

   Viene visualizzata la pagina Elenco credenziali.

2. Fare clic su Crea Nuovo.

   Viene visualizzata la pagina Crea Nuove credenziali.

3. Completare i campi seguenti in modo appropriato:

   Simbolo

   Specifica l'ID univoco per identificare facilmente le credenziali durante una ricerca.

   Userid

   Specifica il nome utente per accedere al percorso UNC. L'utente può essere un utente locale o di dominio Windows con accesso al server di Service Desk.

   Password

   Specifica la password per accedere al percorso UNC.

   Attivo

   Specifica se le credenziali UNC sono attive. Non è possibile utilizzare le credenziali non attive.

4. Fare clic su Salva.

   Le credenziali UNC sono state create.

Creazione di una cartella

Le cartelle vengono utilizzate per organizzare i documenti nei repository. Ad esempio, è possibile creare una cartella Immagini errore sotto il repository Immagini. Questa cartella può contenere tutte le snapshot dei messaggi per gli errori riscontrati dall'utente. Non è possibile creare una cartella per il tipo di repository allegati di Service Desk.

Procedere come descritto di seguito:

1. Selezionare Libreria allegati, Repository nella scheda Amministrazione.

   Viene visualizzata la pagina Elenco repository.

2. Fare clic con il pulsante destro del mouse sul repository in cui si desidera creare la cartella e selezionare Aggiungi cartella.

   Viene visualizzata la pagina Crea Nuova cartella.

3. Immettere il nome della cartella e una descrizione del suo contenuto.

4. Selezionare la scheda Autorizzazioni e specificare i diritti di accesso (a pagina 465) appropriati.

5. Fare clic su Salva.

   Viene creata la cartella.

Diritti di accesso

È possibile aggiungere i diritti di accesso seguenti alla cartella nel repository:

Eredita da padre

Indica che la cartella ha le stesse impostazioni di autorizzazione della cartella padre. Questa opzione viene visualizzata solo per le cartelle secondarie.

Controllo per Gruppo

Indica l'accesso in lettura o in scrittura alla cartella per gruppi specificati. Questa opzione viene visualizzata per tutte le cartelle e le cartelle secondarie.

Concedi autorizzazione in scrittura a tutti

Indica che tutti gli utenti hanno accesso in scrittura alla cartella.

Concedi autorizzazione in lettura a tutti

Indica che tutti gli utenti hanno accesso in lettura alla cartella. L'autorizzazione in lettura indica che è possibile visualizzare la cartella ma non modificarla, eliminarla o memorizzare in essa dei file. Gli utenti con diritti di amministratore possono modificare una cartella anche se il gruppo con autorizzazione loro associato non può farlo. Se un utente appartiene a più gruppi con autorizzazione con diversi livelli di accesso al documento, ottiene il livello di accesso più alto disponibile (ad esempio, se un gruppo dispone di accesso in sola lettura e l'altro di accesso in scrittura, l'utente ottiene l'accesso in scrittura).

Nota: Se si seleziona la casella di controllo Concedi autorizzazione in scrittura a tutti, viene selezionata automaticamente la casella di controllo Concedi autorizzazione in lettura a tutti.

Gruppi disponibili

Visualizza tutti i gruppi. È possibile scegliere i gruppi da questo elenco. Ad esempio, selezionare un gruppo e fare clic su > per Gruppi con autorizzazione di scrittura per fornire a tutti gli utenti compresi in tale gruppo l'accesso in lettura e scrittura alla cartella. Utilizzare Mostra filtro per specificare i criteri e filtrare i gruppi.

Annunci

È possibile utilizzare CA SDM per pubblicare un annuncio per gli utenti. Gli annunci consentono di ridurre il numero di chiamate in arrivo e di aumentare la produttività grazie alla risoluzione dinamica dei ticket e alla possibilità di comunicare informazioni importanti a tutti gli utenti interessati. Gli utenti possono scorrere più annunci memorizzati.

Nota: gli annunci sono validi per tutti i modelli di service desk.

È possibile aggiungere nuovi annunci e aggiornare quelli esistenti. Gli annunci fanno parte della funzione dei dati di riferimento di CA SDM, pertanto tramite il tipo di accesso è possibile controllare quali contatti possono crearli.

Un annuncio può specificare uno o entrambi i seguenti elementi:

Posizione

Specifica una posizione fisica, ad esempio una città, un edificio o un piano di un edificio.

Organizzazione

Specifica un ID di organizzazione. Se un'organizzazione è impostata per un annuncio, solo gli individui assegnati all'organizzazione possono visualizzarlo.

Quando per un annuncio è impostato Posizione o Organizzazione, solo i contatti nella specifica posizione o organizzazione lo riceveranno. Qualsiasi contatto può visualizzare tutti gli annunci che non hanno limitazioni di posizione o organizzazione. Ad esempio, se nessuna delle due è impostata, i contatti in qualsiasi posizione e organizzazione possono visualizzare l'annuncio.

Nota: è possibile specificare gli annunci utilizzando la funzione di amministrazione dell'interfaccia Web. Per informazioni sulla definizione degli annunci, consultare la *Guida in linea*.

Ulteriori informazioni:

Visibilità degli annunci interni (a pagina 466)
Definizione dell'urgenza degli annunci (a pagina 467)

Visibilità degli annunci interni

È possibile controllare se un annuncio è visibile agli utenti interni utilizzando la casella di controllo Interna nella pagina Crea nuovo annuncio. L'impostazione Visualizzare i registri interni del tipo di accesso per l'utente collegato determina se un utente può visualizzare gli elementi contrassegnati come interni.

Definizione dell'urgenza degli annunci

È possibile specificare l'urgenza di un annuncio registrato.

Per specificare l'urgenza degli annunci

1. Creare un annuncio o accedere alla pagina Dettagli annuncio per modificare un annuncio esistente.
2. Selezionare uno dei seguenti valori dall'elenco a discesa Tipo annuncio:

   Routine

   Il testo viene visualizzato in nero.

   Consulenza

   Il testo viene visualizzato in arancione.

   Emergenza

   Il testo viene visualizzato in rosso.

   Fare clic su Salva.

   L'annuncio registrato è contrassegnato con colori diversi nella pagina Elenco annunci.

Configurazione delle query memorizzate

CA SDM supporta l'uso di query memorizzate per la produzione di due tipi di dati:

- Le query del contatore consentono di personalizzare il contatore dell'interfaccia Web mediante l'aggiunta di campi del contatore per gli elementi desiderati.
- Le query dei KPI consentono di recuperare informazioni cronologiche su un periodo specifico del valore di un contatore, in modo da utilizzarle per il reporting basata sul Web.

Le query memorizzate sono valide per tutti i modelli di service desk. le query memorizzate non hanno lo scopo di condurre gli utenti in una nuova pagina.

Sono gli amministratori che definiscono le query memorizzate disponibili agli utenti. È possibile utilizzare le query memorizzate predefinite che sono installate in CA SDM oppure definirne altre. È possibile definire query memorizzate utilizzando la funzione di amministrazione dell'interfaccia Web.

Prendere in considerazione le seguenti informazioni sulle definizioni delle query memorizzate:

- Una clausola valida per la query memorizzata è integrata in un'istruzione SELECT appropriata e passata al relativo motore DBMS per l'elaborazione. Per sviluppare le istruzioni SELECT, consultare i file di definizione oggetto nelle directory seguenti:
  - Windows: directory-installazione\bopcfg\majic
  - UNIX: $NX_ROOT/bopcfg/majic
- Le query memorizzate utilizzano le istruzioni di oggetti e attributi per la creazione della clausola SQL WHERE anziché i nomi di campo a livello di database.
- CA SDM non supporta le unioni cartesiane per le query memorizzate. Per garantire che la query memorizzata non produca un'unione cartesiana, immettere il comando riportato di seguito in base al sistema in uso.
  - Windows: bop_cmd -f *directory_installazione*\bopcfg\interp\bop_diag.frg "check_queries()"
  - UNIX: bop_cmd -f $NX_ROOT/bopcfg/interp/bop_diag.frg "check_queries()"

  Aggiornare le query che vengono contrassegnate dopo l'esecuzione del comando per evitare unioni cartesiane.
- La query memorizzata URL è un'opzione disponibile durante la creazione delle query memorizzate. La query memorizzata URL esegue una query e restituisce risultati numerici validi solo con Gestione della conoscenza.

Nota: per ulteriori informazioni sulla sintassi di definizione degli oggetti, consultare la *Guida di riferimento tecnico*. Per ulteriori informazioni su come definire le query memorizzate, consultare la *Guida in linea*.

Numeri di sequenza

Quando un ticket viene aperto, gli viene automaticamente assegnato il successivo numero di sequenza disponibile. Ad esempio, se l'ultima richiesta aperta è la numero 5, alla successiva viene assegnato il numero 6.

Importante Dopo l'installazione di una nuova versione di CA SDM, l'ID record interno per tutti i ticket viene reimpostato su 1. Per garantire che non vengano creati ID record duplicati, non creare ticket prima di aver ripristinato eventuali dati di backup.

È possibile personalizzare la modalità di numerazione delle richieste, degli ordini di cambiamento e delle questioni includendo nei relativi schemi di numerazione un prefisso o un suffisso univoco. Ad esempio, per tenere traccia delle richieste per mese, è possibile aggiungere un identificativo di mese come prefisso o come suffisso allo schema di numerazione della richiesta.

Nota: per informazioni su come personalizzare i numeri assegnati ai ticket utilizzando la funzione amministrativa dell'interfaccia Web, consultare la *Guida in linea*.

Poiché per ogni tipo di ticket viene definito uno schema di numerazione separato, impostare gli schemi di numerazione per tutti i modelli di service desk. È possibile controllare Il formato della numerazione delle richieste, degli ordini di cambiamento e delle questioni modificando le impostazioni relative al numero di sequenza. Per impostazione predefinita, i nuovi ticket vengono numerati utilizzando valori interi consecutivi. Poiché il campo relativo al numero di un ticket è di tipo string e non numerico, assegnare valori aggiuntivi di tipo string da utilizzare come prefissi o suffissi quando viene generato il numero per un nuovo ticket. Ad esempio, è possibile specificare r:, c: e i: per i prefissi relativi a richieste, ordini di cambiamento e incidenti. Grazie a questa configurazione, l'utente può facilmente distinguere i vari tipi di ticket senza fare confusione.

Incidenti e Problemi condividono gli schemi di numerazione con le Richieste in quanto, a livello interno, gli Incidenti e i Problemi vengono considerati come tipi di Richiesta.

Uso del registro di audit

CA SDM crea un registro di audit in cui vengono memorizzate le informazioni seguenti:

- Tutte le modifiche apportate a una Questione (Issue)
- Tutte le modifiche apportate a una Richiesta (Call_Req)
- Tutte le modifiche apportate a un Ordine di cambiamento (Change_Request)
- Tutte le modifiche apportate a una partizione dati (Domain)
- L'ID di accesso della persona associata al Cambiamento e il giorno/data/data e ora di sistema associati.
- I valori precedenti e successivi dell'aggiornamento, dell'inserimento o dell'eliminazione.
- La creazione di contatti
- Le attività di creazione e aggiornamento dell'oggetto nr

Nota: il registro di audit acquisisce solo le modifiche al campo della partizione dati del contatto e nessun altro aggiornamento al record di contatto.

La funzione Registro di audit è installata automaticamente. Per attivarla, occorre installare due opzioni del registro di audit mediante Gestione opzioni: audit_ins e audit_upd. Dopo aver installato queste opzioni, è possibile accedere al registro di audit dalla scheda Amministrazione selezionando Service Desk, Elenco registri di audit. È possibile effettuare una ricerca in Elenco registri di audit tramite uno strumento di ricerca integrato per facilitare la creazione del report.

Nota: per informazioni sull' installazione e l'impostazione dei valori delle opzioni, consultare la *Guida in linea*.

Integrazione con CA Network and Systems Management

È possibile definire i record messaggio di gestione eventi e le azioni associate ai record messaggio in CA NSM per creare automaticamente nuove richieste, allegare commenti a richieste esistenti o pubblicare annunci in CA SDM.

Nota: per ulteriori informazioni sull'integrazione di CA NSM, consultare la *Guida all'implementazione*.

Stampa di pagine Web CA SDM

CA SDM utilizza immagini di sfondo per i pulsanti e le schede del notebook. Per impostazione predefinita, in molti browser queste immagini di sfondo *non* vengono stampate. Pertanto, se si seleziona File, Stampa nel menu del browser o nel menu di CA SDM, la pagina stampata riporta solo gli angoli dei pulsanti o delle schede.

Per stampare pagine Web di CA SDM utilizzando Internet Explorer

1. Selezionare Strumenti->Opzioni Internet.

   Viene visualizzata la finestra di dialogo Opzioni Internet.

2. Selezionare la scheda Avanzate.
3. Scorrere fino all'intestazione Stampa e selezionare l'opzione Stampa colori e immagini di sfondo.

   Le pagine Web CA SDM stampate includono grafica di sfondo.

Per stampare pagine Web di CA SDM utilizzando Firefox

1. Selezionare File, Impostazione pagina.
2. Selezionare la scheda Formato e opzioni.
3. Selezionare la casella di controllo Stampa sfondo (colori e immagini).

   Le pagine Web CA SDM stampate includono grafica di sfondo.

Blocco dei record nell'interfaccia Web

Quando un utente modifica un record del database utilizzando l'interfaccia Web, assume la proprietà esclusiva del record bloccandolo per due minuti, che è la durata predefinita. È possibile modificare la durata predefinita utilizzando la proprietà ExclLockSeconds nel file web.cfg.

Le seguenti condizioni sono correlate all'aggiornamento di un record di database da parte di un utente:

- Se un utente *ha la possibilità* modificare e inviare le modifiche entro un tempo prestabilito, le modifiche vengono incluse nel database.

  Durante il periodo di tempo in cui il database rimane bloccato, altri utenti (sia Web che non Web) possono accedere al record in lettura ma non in scrittura. Se un altro utente tenta di modificare il record mentre è bloccato, viene visualizzato un messaggio di errore.

- Se un utente *non ha la possibilità* di modificare e inviare le modifiche entro un tempo prestabilito, il blocco del record decade automaticamente e altri utenti possono modificarlo.

  Quando l'utente invia gli aggiornamenti, vengono controllate la data e l'ora per assicurare che nessun altro abbia modificato il record, e avviene quanto segue:

  - Se il record non è stato modificato dalla rimozione del blocco esclusivo, gli aggiornamenti dell'utente vengono salvati nel database.
  - Se un altro utente ha invece modificato il record dopo la scadenza del blocco, l'utente riceve un messaggio di errore quando tenta di effettuare il salvataggio e le modifiche non vengono salvate. L'utente deve riavviare il processo e immettere nuovamente le modifiche.

Ulteriori informazioni:

Modifica del file di configurazione (a pagina 538)

Struttura di supporto

La *struttura di supporto* del service desk è costituita dai componenti necessari agli utenti per la risoluzione dei problemi. È possibile configurare la struttura di supporto di CA SDM in base al proprio modello di supporto (interno, esterno o entrambi).

Nota: è possibile personalizzare le Issue, le Richieste e gli Ordini di cambiamento in base alle specifiche esigenze del sito. Per ulteriori informazioni, consultare la *Guida all'implementazione* e la *Guida in linea*.

Abilitazione della Guida in linea di CAPA

CA Productivity Accelerator (CAPA) fornisce il supporto sensibile al contesto delle prestazioni all'interno delle applicazioni per i moduli Web degli analisti di CA SDM. Il pacchetto di CAPA viene integrato direttamente nei menu della Guida sensibile al contesto delle pagine Web degli analisti di CA SDM. L'integrazione del contenuto della Guida in linea di CAPA con CA SDM avviene mediante gli script dei menu della Guida in linea. Questi script avviano il contenuto registrato della Guida in linea di CAPA dagli elenchi a discesa dal menu della Guida in linea di CA SDM e dalla Guida in linea di scelta rapida sensibile al contesto.

Nota: questo argomento non include informazioni sullo strumento di registrazione CAPA, su come ottenere e configurare il contenuto della Guida in linea di CAPA e su come installare la guida in linea intelligente.

CA SDM fornisce un ID univoco per riconoscere ciascun modulo Web in modo univoco. Se un elemento di identificazione è presente nel frame superiore di CA SDM, lo strumento di registrazione CAPA è in grado di riconoscere un modulo di applicazione Web. Una volta che il frame superiore viene riconosciuto, tutti i sottoframe vengono considerati parte dell'applicazione. È necessario identificare anche i sottoframe che vengono caricati da un dominio diverso; in caso contrario non vengono considerati parte di CA SDM. Per abilitare la Guida in linea di CAPA, è necessario per preparare il contenuto della guida, quindi configurare le opzioni per avviare la Guida in linea di CAPA.

Nota: per personalizzare i file HTML, utilizzare i metodi di richiamo dai file ias_helper.js affinché il registratore CAPA riconosca i moduli HTML.

La Guida in linea di CAPA non è supportata nelle interfacce Dipendente, Cliente o PDA di CA SDM. Per ulteriori informazioni sui browser che supportano CAPA, consultare la documentazione CAPA.

Procedere come descritto di seguito:

1. Aprire il file capa.properties dalla seguente directory di CA SDM:

   ```
   %NX_ROOT/bopcfg/www/wwwroot
   ```

2. Cambiare i valori seguenti nel file:

   - Enable_Alerts = 0. Questa opzione verifica e visualizza i messaggi di avviso JavaScript in una console del browser quando la pagina Web di CA SDM viene caricata.

3. Salvare il file.

4. Accedere al file web.cfg nella directory di CA SDM, aggiungere DebugScript=1 e riavviare il motore Web.

   Il contenuto registrato viene preparato, pubblicato e distribuito sul server CAPA.

5. Aprire il file capa.properties e cambiare i valori seguenti:

   - Enable_For_Recording = 0
   - Show_Learn_Links = 1. Questo valore mostra l'opzione Guida in linea di CAPA nel menu della Guida in linea di CA SDM e nel menu di scelta rapida della Guida in linea.
   - Server_Name = nome del server in cui è distribuito il contenuto pubblicato di CAPA.
   - Server_Port = porta del server CAPA in cui è distribuito il contenuto pubblicato di CAPA. Ad esempio, la porta TOMCAT.
   - Virtual_Dir = directory virtuale in cui il contenuto pubblicato di CAPA è distribuito sul server CAPA.
   - Namespace = spazio dei nomi del contesto dell'applicazione. Ad esempio, app.SDM.Project123;en.
   - Enable_Alerts = 0

6. Salvare il file.

   Ora è possibile avviare la Guida in linea di CAPA dai moduli Web degli analista di CA SDM.

Capitolo 11: Controllo del comportamento del sistema

Questa sezione contiene i seguenti argomenti:

Utilizzo di Gestione opzioni (a pagina 475)

Utilizzo di Gestione opzioni

Il client Web CA SDM consente di utilizzare Gestione opzioni della scheda Amministrazione per le seguenti azioni:

- Ottenere un elenco di tutte le opzioni disponibili
- Visualizzare un riepilogo di ciascuna opzione, ad esempio l'applicazione a cui è associata, una breve descrizione e lo stato.
- Visualizzare i dettagli di opzioni specifiche

  Quando si visualizzano le informazioni dettagliate di un'opzione, è possibile ottenere una descrizione completa sulla funzionalità dell'opzione nella *Guida in linea*. La descrizione presente nella *Guida in linea* include le azioni specifiche da eseguire per la modifica dell'opzione. Ad esempio, dopo l'installazione o la disinstallazione di determinate opzioni, verificare di aver riavviato il server di CA SDM affinché l'opzione venga applicata. Questo passaggio è indicato anche nella descrizione della *Guida in linea*.

- Esaminare lo stato di tutte le opzioni a livello di riepilogo
- Disinstallazione di un'opzione disponibile (applicabile solo sul server in background)

  Molte delle opzioni sono preconfigurate e installate durante l'installazione di CA SDM. L'utilizzo di Gestione opzioni per installare o disinstallare opzioni può alterare alcune o tutte le impostazioni predefinite.

- Installazione di un'opzione definita (applicabile solo sul server in background)

Nota: nei cicli di rilascio, le opzioni vengono occasionalmente rese disponibili tramite il supporto di CA SDM in risposta alle richieste degli utenti. Per ulteriori informazioni su queste opzioni, contattare il supporto di CA SDM. Per ulteriori informazioni su come utilizzare Gestione opzioni, consultare la *Guida in linea*.

Modalità di modifica dell'ambiente di sistema

CA SDM utilizza variabili di ambiente specificate nel file modello di ambiente (NX.env.tpl) per determinare specifici comportamenti. È possibile utilizzare variabili di ambiente per modificare alcuni comportamenti del sistema. Solitamente, si utilizza Gestione opzioni per controllare il comportamento del sistema. Tuttavia, il supporto tecnico di CA richiede di modificare direttamente una particolare variabile di ambiente.

Quando si modifica un file modello di ambiente, tenere conto di quanto segue:

- Le variabili di ambiente impostate in questo file possono essere sostituite impostando la variabile di ambiente nell'area di elaborazione in cui viene eseguito un processo. Sebbene questa configurazione sia conveniente in alcuni casi, in genere non è consigliabile. Una variabile impostata con il prefisso @ non può essere sostituita da un'altra variabile nell'area di esecuzione dei processi. A meno che non esista un motivo specifico per cui una variabile di ambiente possa essere configurata come sostituibile, il nome della variabile è sempre preceduto dal simbolo @ nel file modello.
- I caratteri per definire un commento in questo file sono cancelletto (#) e punto esclamativo (!). Il punto esclamativo viene utilizzato anche per disattivare un'opzione.

Importante: Modificare il file modello (NX.env.tpl) e lasciare che il processo di configurazione applichi le modifiche al file di ambiente. Non modificare mai direttamente il file di ambiente (NX.env).

Procedere come descritto di seguito:

1. Backup del file modello di ambiente (.tpl) corrispondente al proprio ambiente di sistema:
   - UNIX—$NX_ROOT/pdmconf/NX.env.tpl.
   - Windows—installation-directory\pdmconf\NX.env_nt.tpl.
2. Modificare il file di esempio dell'ambiente sul server seguente, a seconda della configurazione di CA SDM:
   - Convenzionale: server primario
   - Disponibilità avanzata: un server di standby

   Nota: È possibile visualizzare e modificare questo file utilizzando un qualsiasi editor di testo. Per modificare il file, gli utenti Windows devono utilizzare WordPad.
3. Apportare le modifiche indicate dal supporto tecnico e salvarle.
4. Eseguire l'utilità di configurazione sull'installazione del server primario o del server di standby per applicare al file di ambiente effettivo le modifiche apportate al file di esempio dell'ambiente.

   Nota: per informazioni su come eseguire l'utilità di configurazione, consultare la *Guida all'implementazione.*

5. A seconda della configurazione di CA SDM, completare una delle azioni seguenti:
   - Convenzionale: arrestare e riavviare il server primario per applicare le modifiche apportate al file di ambiente.
   - Disponibilità avanzata: riavviare tutti i server di CA SDM (a pagina 49).

   Nota: Per non arrestare il sistema, il supporto tecnico può richiedere di riavviare solo determinati processi anziché l'intero server di CA SDM.

Eventi

È possibile configurare eventi assegnati a oggetti per eseguire azioni configurate. Gli eventi sono procedure eseguite allo scadere di un periodo di tempo specificato. Ad esempio, un evento consente di inviare un messaggio all'analista di Service Desk se una Issue con priorità 1 non viene ricevuta entro un'ora. Altre parti del sistema utilizzano eventi, ad esempio i Tipi servizio.

È possibile definire eventi per Richieste, Incidenti, Problemi, Ordini di cambiamento, Issue, contatti, elementi della configurazione e titolari globali e specifici. La data e ora di esecuzione degli eventi viene pianificata in base a ritardo e turno.

Nota: per ulteriori informazioni sugli eventi, consultare la *Guida in linea*.

Macro

Le macro sono script di piccole dimensioni che definiscono le condizioni o le azioni. Quando gli eventi vengono eseguiti o si verificano determinati comportamenti, è possibile che vengano eseguite una o più macro azioni. Prima dell'esecuzione delle macro, è possibile utilizzare una macro condizionale per determinare quale set di macro azioni attivare.

È possibile utilizzare macro nelle seguenti aree:

- Eventi
- Modelli di comportamento per Issue oppure Ordini di cambiamento
- Notifiche delle attività

Il prodotto include diverse macro. Gli utenti possono inoltre crearne di ulteriori.

Nota: i clienti non possono aggiungere macro di tipo Azione o Condizione ma possono creare macro condizionali semplici con condizioni definite in locale. Le condizioni definite in locale sono macro non complesse che possono essere create dalle finestre della GUI e non sostituiscono le macro di tipo Condizione.

Per ogni macro è necessario specificare il tipo di oggetto che essa deve utilizzare. Se si crea una macro condizionale definita in locale per il controllo dei valori delle richieste, è necessario impostare il tipo su Richiesta. Quando si selezionano macro per eventi e comportamenti, CA SDM visualizza solo le macro di tipo corrispondente al tipo di evento o di comportamento.

Tipi macro

Ognuna delle macro seguenti appartiene a un tipo specifico di macro che ne descrive l'uso:

Azione

Esegue determinate azioni, ad esempio l'incremento del livello di priorità di una Issue.

Associa evento

Associa un oggetto evento a un Cambiamento, una Issue, una Richiesta, un contatto o un elemento della configurazione.

Condizione

Valuta alcune condizioni di tipo true o false.

Esegui azione CA IT PAM

Esegue un'azione CA IT PAM. CA IT PAM è un motore di flusso di lavoro che consente la gestione e l'esecuzione di report su gruppi di attività che possono richiedere approvazioni elettroniche.

Esegui azione CA Workflow

Esegue un'azione CA Workflow. CA Workflow consente di gestire processi di flusso di lavoro nel proprio ambiente, come ad esempio il monitoraggio delle attività completate relative a ticket associati a una specifica categoria o area.

Riferimento remoto

Avvia un programma esterno sul server.

Più notifiche

Invia una notifica a uno o più contatti. Questa macro è particolarmente utile poiché consente di specificare il messaggio, i destinatari e il livello di urgenza.

Condizione Site-Defined

Crea eventi basati su condizioni di tipo true o false, sulla base di attributi del ticket per l'applicazione dei livelli di servizio. Ad esempio, è possibile creare una macro di tipo Condizione che corrisponde a true se una richiesta ha priorità 1 e non è ancora assegnata. Può essere associata a un evento che viene eseguito subito dopo la creazione di una richiesta.

Uso delle macro con gli eventi

Nei dettagli di un evento, è possibile specificare una macro condizionale per il campo Condizione evento. Inoltre, nelle colonne Esegui in true ed Esegui in false, è possibile specificare un numero qualsiasi di macro, tranne quelle condizionali. Quando l'evento viene attivato, innanzitutto viene valutata la macro condizionale. Se la valutazione restituisce un valore true, vengono attivate tutte le macro della colonna True. Se la valutazione restituisce un valore false, vengono attivate tutte le macro della colonna False. Inoltre, la macro condizionale può verificare l'impostazione dell'assegnatario, il livello di priorità, la violazione del tipo di servizio e così via. Se non è specificata alcuna macro di tipo Condizione evento, l'evento esegue automaticamente le macro della colonna True.

Nei dettagli di un evento, è possibile selezionare quasi tutti i tipi di macro per la notifica ai contatti, impostare i valori nell'oggetto contesto, eseguire un riferimento remoto o associare un altro evento.

Uso delle macro nel comportamento delle categorie questione e modifica

Le macro possono anche essere utilizzate per il comportamento delle categorie questione e modifica. Nella scheda Flusso di lavoro dei dettagli di una categoria, è possibile selezionare uno stato del flusso di lavoro. Nei dettagli del flusso di lavoro, fare clic sul pulsante Comportamento. Come per l'evento, è possibile impostare una condizione e le azioni risultanti.

Nella scheda Transizione dei dettagli comportamento, è possibile specificare una macro condizionale per determinare se è possibile modificare lo stato dell'attività. Questo evento viene attivato quando un utente tenta di modificare lo stato dell'attività dal valore corrente a un altro valore. Se la condizione restituisce un valore false, l'aggiornamento dello stato non è consentito.

Le reali attività del flusso di lavoro vengono create dai modelli presenti nel modello della categoria. Quando il valore dello stato di un'attività viene modificato e salvato, il comportamento specificato nel modello della categoria viene attivato, ovvero la condizione e le azioni risultanti vengono eseguite.

Nota: usare una macro di tipo Associa evento per associare un evento a un'attività del flusso di lavoro.

Utilizzo di macro con più notifiche

Più notifiche

Il corpo del messaggio della notifica multipla punta direttamente alla tabella dell'oggetto selezionato. Pertanto, quando si fa riferimento a campi nella tabella dell'oggetto, CR (Call_Req) ad esempio, è possibile fare riferimento al nome dell'attributo del campo. Se si desidera fornire la descrizione del ticket Richiesta chiamata, digitare la stringa indicata di seguito nel testo del messaggio:

```
Descrizione: @{description}
```

Una QREL (Query Relation) è una relazione che contiene un elenco di oggetti definiti da una clausola SQL WHERE. È possibile aggiungere una relazione QREL alla descrizione di una macro per notifiche multiple. Se si desidera inserire la relazione QREL nella descrizione per act_log QREL <-- alg, è possibile utilizzare la stringa indicata di seguito in una macro per le notifiche:

```
@{act_log.0.description}
```

È possibile utilizzare variabili di sostituzione per rendere i messaggi di notifica più rilevanti e dinamici. Queste variabili utilizzano il formato @{attribute_path_here} dove attribute_path_here è un attributo di un oggetto CA SDM. Quando la notifica viene inviata, la variabile viene sostituita con il valore di attributo specificato.

Una notifica, sia che provenga da un registro attività o da una notifica multipla, ha sempre un contesto di base, ovvero un punto di riferimento, che solitamente è rappresentato da un ticket o da un'attività del flusso di lavoro. Nelle notifiche multiple, l'oggetto base viene specificato dal campo del tipo di macro Notifica. Per fare riferimento a qualsiasi attributo in tale oggetto si utilizza la sintassi @{}.

Esempio: una notifica multipla di tipo Richiesta fa riferimento a qualsiasi attributo nell'oggetto 'cr' (Call_Req). Per includere la descrizione della richiesta, specificare @{description}. Per i riferimenti ad altri oggetti, viene utilizzata la notazione a punti. Ad esempio, per includere il cognome dell'assegnatario della richiesta: @{assignee.last_name}.

Utilizzo di macro con una condizione definita dal sito

Condizione definita dal sito

La macro condizionale è composta da una o più condizioni *atomic*. Ogni condizione atomic verifica il valore di un singolo attributo. Pertanto, se l'utente desidera che venga eseguita un'azione in base ai valori di Assegnatario e Categoria, la macro condizionale utilizzerà probabilmente due condizioni atomic, una per il valore di Assegnatario e una per il valore di Categoria. Quando si utilizza una macro condizionale in un evento, le singole condizioni atomic vengono collegate tramite un operatore booleano, principalmente 'AND' oppure 'OR'.

Dettagli macro condizionale riporta un elenco di condizioni atomic, la cui lettura avviene da sinistra a destra nel modo seguente:

Attributo	**Operatore**	**Valore**	**Operatore logico**	**Significato**
Assegnatario	Uguale	Jones	E	L'assegnatario è Jones e...
Costo	Minore di	600	oppure	Il costo è un valore intero minore di 600 o...
Gruppo	Empty/NULL		E	Il campo Gruppo è vuoto.

Nota: gli operatori logici (AND, OR) collegano due condizioni atomic. Quando sono presenti due condizioni atomic, ad esempio 1 e 2, il collegamento avviene tramite la condizione atomic 1. La condizione atomic 2 non viene utilizzata. Inoltre, in alcuni casi la selezione di determinati operatori non è utile, ad esempio, non ha senso utilizzare l'operatore *Minore di* se l'attributo è *Assegnatario*. Per ulteriori informazioni su come creare macro condizionali, consultare la *Guida in linea*.

Capitolo 12: Configurazione dell'assegnazione automatica

Questa sezione contiene i seguenti argomenti:

Assegnazione automatica (a pagina 483)
Relazioni di assegnazione automatica (a pagina 484)
Metodi di assegnazione automatica (a pagina 484)
Modalità di avvio dell'implementazione dell'assegnazione automatica (a pagina 485)
Gruppo e assegnatario predefiniti (a pagina 491)
Abilitazione dell'assegnazione automatica (a pagina 491)
Sostituzione dell'assegnazione automatica (a pagina 492)
Controlli di assegnazione (a pagina 493)
Registro attività (a pagina 496)
Abilitazione della registrazione delle attività per gli attributi aggiuntivi (a pagina 497)
Tracciamento dell'assegnazione automatica (a pagina 497)
Query memorizzate (a pagina 498)
Modalità di assegnazione automatica dei ticket (a pagina 498)
Assegnazione automatica delle attività flusso di lavoro (a pagina 505)
Assegnazioni automatiche basate sull'elemento della configurazione (a pagina 509)

Assegnazione automatica

Assegnazione automatica di CA SDM può ridurre notevolmente il tempo necessario per la gestione dei ticket mediante l'automazione del relativo processo di assegnazione agli analisti. L'automazione consente di rendere più efficaci le attività associate al bilanciamento dei carichi di lavoro e al coordinamento delle pianificazioni di lavoro.

È possibile configurare l'assegnazione automatica per assegnare i ticket in base ai seguenti fattori:

- I gruppi di analisti che lavorano sui ticket o sulle attività
- Quando è necessario eseguire il lavoro
- Le sedi che prestano assistenza ai clienti interessati
- Il carico di lavoro e la disponibilità di ogni analista
- Il valore di un attributo di un elemento di configurazione associato al ticket

  Nota: l'assegnazione automatica basata sugli elementi della configurazione (a pagina 509) consente di creare assegnazioni specifiche del gruppo solo per i ticket di tipo Richiesta/Incidente/Problema.

Non occorre implementare l'assegnazione automatica in un'unica fase. È possibile sviluppare una strategia per implementarla a fasi e in modo graduale. È ad esempio possibile abilitare la funzione dapprima solo per i tipi di ticket, i gruppi di analisti o le posizioni selezionati.

Relazioni di assegnazione automatica

Il processo di assegnazione automatica può riguardare diversi elementi di CA SDM. Di seguito sono riportate le relazioni tra gli elementi:

- Aree e categorie con gruppi, posizioni e turni
- Gruppi con posizioni e turni
- Modelli CA Workflow con contatti

Per semplificare l'amministrazione dell'assegnazione automatica, tutte le relazioni possono essere gestite da un qualsiasi elemento correlato. Nel caso ad esempio di una relazione tra un gruppo di analisti e una categoria di cambiamenti è possibile gestire l'associazione dalla pagina Dettagli categoria Cambiamento o Dettagli gruppo.

Metodi di assegnazione automatica

Per assegnare i ticket sono disponibili i seguenti metodi di base:

Assegnazione automatica basata sulla posizione

Crea assegnazioni per tutti i tipi di ticket in base a:

- Aree e categorie relative a gruppi, posizioni e turni
- Gruppi relativi a posizioni e turni
- Modelli di flussi di lavoro CA relativi a contatti

Nota: l'assegnazione automatica basata sulla posizione è definita semplicemente assegnazione automatica.

Assegnazione automatica basata sull'elemento della configurazione

Crea assegnazioni a gruppi per ticket di tipo richiesta, problema e incidente in base a:

- Aree relative a ticket associati ad elementi della configurazione
- Attributi di elementi della configurazione utilizzati per registrare informazioni relative a informazioni su contatto/gruppo

L'assegnazione automatica basata sulla posizione e quella basata sull'elemento della configurazione si escludono a vicenda perché è possibile selezionare un solo algoritmo da utilizzare in una data area Richiesta/Incidente/Problema. L'assegnazione automatica basata sulla posizione e i metodi basati sull'elemento della configurazione consentono entrambi di assegnare i ticket al momento della loro creazione, tuttavia l'assegnazione automatica basata sull'elemento della configurazione è distinta poiché rivaluta anche le assegnazioni per un ticket ogni volta che cambia l'Area o l'elemento della configurazione di un ticket Richiesta/Incidente/Problema. Se si specifica l'assegnazione automatica basata sull'elemento della configurazione ma non viene generata alcuna assegnazione a un gruppo per un ticket, viene consultata l'opzione Area_Defaults per stabilire se, per assegnare il ticket, è necessario utilizzare i valori predefiniti Gruppo e Assegnatario.

Modalità di avvio dell'implementazione dell'assegnazione automatica

Seguire le linee guida riportate di seguito per avviare l'implementazione dell'assegnazione automatica per gli analisti e i gruppi di analisti selezionati:

1. Identificare una o più aree o categorie per le quali abilitare l'assegnazione automatica.

   Nota: per verificare le configurazioni delle categorie e delle aree del sito, esaminarne le impostazioni nell'interfaccia Web di CA SDM. Per istruzioni, vedere la *Guida in linea*.

2. Per impostazione predefinita, l'assegnazione automatica è disabilitata. Attivarla soltanto per le aree e le categorie (a pagina 485) che si desidera utilizzare.
3. Creare le relazioni tra un'area o una categoria specifica e i gruppi di analisti (a pagina 486) idonei per l'assegnazione dei ticket all'interno dell'area o della categoria.
4. Contrassegnare i singoli membri dei gruppi di analisti (a pagina 486) come disponibili.

Aree e categorie

Nota: quando si configurano aree e categorie, è buona norma impostare gruppi e assegnatari predefiniti (a pagina 491).

Per configurare l'assegnazione automatica per i ticket di tipo richiesta, incidente e problema, utilizzare i seguenti controlli della scheda Assegnazione automatica della pagina Dettagli area Richiesta/Incidente/Problema:

- Aggiorna gruppi
- Aggiorna ubicazioni
- Aggiorna turni

Nota: la casella di controllo per l'abilitazione dell'assegnazione automatica è presente anche nella scheda Assegnazione automatica di ognuna di queste pagine. È visibile solo quando la pagina è in modalità di modifica.

Le seguenti pagine dell'interfaccia forniscono gli stessi controlli per la configurazione dell'assegnazione automatica di Issue e Ordini di cambiamento:

- Dettagli categoria Cambiamento
- Dettagli categoria Issue

Gruppi di analisti

Per configurare l'assegnazione automatica è necessario definire almeno le relazioni tra i gruppi di analisti e le aree o le categorie. Gli assegnatari vengono selezionati dai gruppi che soddisfano *tutti* i criteri di assegnazione automatica specificati. Se non vengono definiti vincoli aggiuntivi, i ticket vengono assegnati automaticamente al membro del gruppo con il minor numero di ticket attivi.

Se non vi sono gruppi associati ad un'area o una categoria, vengono assegnati il gruppo e l'assegnatario predefiniti. Se questi valori predefiniti non sono stati definiti, il ticket deve essere assegnato manualmente.

È possibile gestire le relazioni tra i gruppi e le aree o categorie nella pagina dei dettagli delle aree o delle categorie.

In alternativa, è possibile gestire le stesse relazioni nella scheda Assegnazione automatica della pagina Dettagli gruppo utilizzando i seguenti controlli:

- Aggiorna aree Richiesta
- Aggiorna categorie Cambiamento
- Aggiorna categorie Issue
- Aggiorna ubicazioni

Analisti

I campi della pagina Dettagli analista consentono di determinare se l'analista è idoneo per l'assegnazione automatica.

Gli analisti sono idonei per l'assegnazione automatica solo se sono contrassegnati come disponibili.

La pagina Dettagli analista fornisce una casella di controllo Disponibile che consente l'assegnazione automatica.

Fare in modo che gli analisti possano controllare la propria disponibilità per l'assegnazione automatica. È possibile monitorare la disponibilità degli analisti utilizzando le query memorizzate.

Nota: la casella di controllo Disponibile non è da prendere in considerazione durante l'assegnazione automatica delle attività del flusso di lavoro.

Il campo Pianificazione lavoro consente agli analisti di usufruire dell'assegnazione automatica di ticket solo durante i propri turni pianificati. Gli analisti cui non sono state assegnate pianificazioni del lavoro, ma che sono contrassegnati come disponibili, sono sempre idonei per l'assegnazione automatica, purché non presentino altri vincoli che determinano uno stato di non idoneità.

Assegnazione automatica di ticket a un gruppo e non ai contatti presenti nel gruppo

L'assegnazione automatica in CA SDM permette di assegnare ticket ai contatti con l'opzione Disponibile selezionata nel record di contatto. Tuttavia, è possibile assegnare in modo automatico incidenti, questioni, ordini di cambiamento, richieste a un gruppo e non ai contatti presenti in esso. L'opzione NX_AUTOASG_GROUP_ONLY controlla l'assegnazione automatica per i gruppi. Installare questa opzione per assegnare automaticamente i ticket al gruppo invece che ai singoli contatti. NX_AUTOASG_GROUP_ONLY non è disponibile nell'interfaccia Web, ma si installa dal prompt dei comandi.

Procedere come descritto di seguito:

1. Verificare che l'installazione di CA SDM comprenda almeno la patch Versione 12.9 Cumulative 2.
2. Aprire il prompt dei comandi su qualsiasi server di CA SDM.
3. Eseguire il comando riportato di seguito:

   ```
   pdm_options_mgr -c -s AUTOASG_GROUP_ONLY -v 1 -a pdm_option.inst
   ```

   Per impostazione predefinita, le nuove opzioni aggiunte al file nx.env non vengono salvate dopo l'esecuzione di pdm_configure. È possibile salvare le modifiche in via definitiva specificando l'opzione -t come segue:

   ```
   pdm_options_mgr -c -s AUTOASG_GROUP_ONLY -v 1 -a pdm_option.inst -t
   ```

   I comandi aggiornano i file seguenti in CA SDM con la nuova opzione:

   - Windows - NX_ROOT/NX.env e NX_ROOT\pdmconf\nx.env.nt.tpl
   - UNIX/Linux - NX_ROOT/pdmconf/NX.env.tpl

4. Aprire il file NX.env nella cartella di installazione di CA SDM e cercare la variabile @NX_AUTOASG_GROUP_ONLY=1, presente alla fine del file.
5. Aprire il file nx.env.nt.tpl compreso in NX_ROOT/pdmconf e cercare l'opzione @NX_AUTOASG_GROUP_ONLY=1.
6. Riavviare il servizio Daemon Server di CA SDM.

   CA SDM assegna automaticamente i ticket solo al gruppo.
7. Riavviare i server di CA SDM (a pagina 49).

Assegnazione automatica in base alla posizione

Se l'area di servizio è di grandi dimensioni e costituita da molte posizioni che offrono assistenza a diverse community di clienti, è possibile utilizzare la posizione come fattore discriminante per configurare l'assegnazione automatica.

- **Posizione assegnata a un'area o a una categoria**—Assegnando una posizione a un'area o a una categoria, i ticket dell'area o della categoria vengono assegnati automaticamente soltanto se viene trovata una posizione corrispondente. Ad esempio, un ticket di richiesta è assegnato automaticamente se esiste un analista idoneo nelle seguenti posizioni:
  1. Posizione dell'asset interessato
  2. Posizione del cliente interessato

  Se l'asset o il cliente interessato non ha una posizione specifica, la richiesta è assegnata al gruppo o all'assegnatario predefinito. In assenza di queste impostazioni predefinite, la richiesta è lasciata all'assegnazione manuale. È possibile utilizzare le pagine dei dettagli dell'area o della categoria per gestire le relazioni tra le posizioni e le aree o categorie.
- **Posizione assegnata a un gruppo**—Se si associa una posizione a un gruppo, solo i suoi membri sono idonei per l'assegnazione automatica di ticket che riguardano la posizione. È possibile utilizzare le pagine dei dettagli del gruppo per gestire le relazioni tra i gruppi e le posizioni.

Per gestire le relazioni delle posizioni con aree, categorie o gruppi, utilizzare i seguenti controlli nella scheda Assegnazione automatica della pagina Dettagli posizione:

- Aggiorna aree Richiesta
- Aggiorna categorie Cambiamento
- Aggiorna categorie Issue
- Aggiorna gruppi

Esempi: Utilizzo della posizione per configurare l'assegnazione automatica

Di seguito sono riportati esempi del possibile utilizzo della posizione nella configurazione dell'assegnazione automatica:

- **Assegnazione automatica di ticket a una posizione specifica**—I ticket che provengono da altre posizioni vengono associati all'assegnatario e/o al gruppo predefinito oppure vengono destinati all'assegnazione manuale. Ad esempio, potrebbero esistere molti utenti impiegati presso la sede principale della società e altri gruppi di utenti impiegati presso le filiali regionali. Un gruppo di analisti ubicato nella sede principale fornisce assistenza agli utenti locali, mentre i gruppi di analisti mobili visitano le filiali regionali. È possibile configurare l'assegnazione automatica dei ticket solo agli analisti nella sede principale e assegnare manualmente i ticket agli analisti mobili.
- **Assegnazione automatica dei ticket in base alla posizione di utenti o asset**—È possibile vincolare l'idoneità dell'assegnazione automatica a gruppi di analisti che si trovano nelle posizioni dell'utente o dell'asset interessato. Ad esempio, la propria organizzazione dispone di molti uffici e i ticket inviati da ciascun ufficio vengono gestiti solo da gruppi che operano presso tali uffici. È possibile correlare i singoli gruppi alle aree o categorie appropriate *e* alla posizione desiderata. La logica di assegnazione automatica seleziona gli analisti idonei solo dai gruppi che si trovano nella posizione specificata.

Assegnazione automatica in base ai turni

È possibile vincolare l'assegnazione automatica creando una relazione tra un'area o una categoria e un turno. Il turno determina il periodo di tempo entro il quale i ticket sono considerati idonei per l'assegnazione automatica. I ticket aperti al di fuori delle ore del turno vengono assegnati al gruppo e all'analista predefiniti oppure destinati all'assegnazione manuale.

È inoltre possibile utilizzare i turni per controllare l'idoneità dei gruppi e degli analisti per l'assegnazione:

- Se si assegna una pianificazione lavoro ad un gruppo, gli analisti inclusi nel gruppo sono idonei per l'assegnazione automatica solo ai ticket aperti durante la propria pianificazione.

  Nota: il turno di un gruppo viene specificato nel campo Pianificazione lavoro della pagina Dettagli gruppo.

- Se si assegna una pianificazione lavoro ad un singolo analista, l'analista è idoneo per l'assegnazione automatica ai soli ticket aperti durante la pianificazione lavoro specifica.

  Nota: il turno di un analista viene specificato nel campo Pianificazione lavoro della pagina Dettagli analista.

Durante la creazione dei ticket l'assegnazione automatica tenta di identificare l'analista con il numero minimo di ticket attivi in un gruppo che soddisfa i criteri di idoneità dell'assegnazione. Se non viene identificato un analista appropriato, il ticket viene assegnato al gruppo e all'assegnatario predefiniti. Se questi valori predefiniti non sono stati definiti, il ticket deve essere assegnato manualmente.

Per le attività del flusso di lavoro associate a Ordini di cambiamento o Issue, la funzione Assegnazione automatica utilizza una strategia di selezione ancora più semplice. Gli assegnatari vengono selezionati dai gruppi associati ai modelli flusso di lavoro. Gli assegnatari delle attività del flusso di lavoro possono essere di qualsiasi tipo di contatto, ad eccezione di Gruppo. Quando un'attività passa allo stato In sospeso, la funzione Assegnazione automatica seleziona il contatto con il minor numero di attività correlate a Ordini di cambiamento o Issue assegnate. Per evitare risultati indesiderati, se la categoria padre dell'Ordine di cambiamento o della Issue non è abilitata per l'assegnazione automatica, le attività non vengono assegnate automaticamente. Poiché le attività del flusso di lavoro possono includere persone esterne al service desk, potrebbero non essere affidabili per verificare la disponibilità mediante il flag Disponibile.

Nota: l'assegnazione automatica delle attività del flusso di lavoro non valuta il flag Disponibile e non è disponibile per le categorie configurate per l'utilizzo di CA Workflow.

È possibile utilizzare le pagine dei dettagli dell'area o della categoria per correlare un turno ad un'area o una categoria oppure utilizzare i seguenti controlli nella pagina Dettagli turno:

- Aggiorna aree Richiesta
- Aggiorna categorie Cambiamento
- Aggiorna categorie Issue

Esempi: Utilizzo dei turni per configurare l'assegnazione automatica

Di seguito sono riportati esempi del possibile utilizzo dei turni nella configurazione dell'assegnazione automatica:

- **Assegnazione automatica al turno attivo**—Se il Service Desk è operativo 24 ore al giorno, si potrebbe scegliere di configurare l'assegnazione automatica in modo che i problemi di interruzione di rete siano assegnati al turno attivo quando viene aperto il ticket.
- **Abilitazione dell'assegnazione automatica solo durante un turno specifico**—Potrebbe essere necessario restringere ulteriormente l'assegnazione automatica dei ticket ad aree o categorie specifiche. Se ad esempio gli analisti di applicazioni di un sito sono operativi durante il turno mattutino, è possibile assegnare automaticamente i problemi relativi alle applicazioni solo durante quel turno.

Gruppo e assegnatario predefiniti

Quando la logica di assegnazione automatica configurata non è in grado di identificare un gruppo o un assegnatario adatto, il ticket viene assegnato al gruppo e all'assegnatario predefiniti. È possibile specificare questi valori predefiniti nei campi Gruppo e Assegnatario delle seguenti pagine dell'interfaccia Web:

- Dettagli area Richiesta/Incidente/Problema
- Dettagli categoria Cambiamento
- Dettagli Issue

Se l'assegnazione automatica non consente di identificare un gruppo o un assegnatario adatto e non sono specificati i valori predefiniti, il ticket deve essere assegnato manualmente.

Abilitazione dell'assegnazione automatica

Sono disponibili opzioni e controlli per configurare l'assegnazione automatica. È possibile controllare se l'assegnazione automatica viene eseguita come illustrato di seguito:

- Per le Richieste, Incidenti e Problemi assegnati all'area specifica, utilizzare la scheda Assegnazione automatica abilitata della pagina Dettagli area Richiesta/Incidente/Problema.
- Per gli Ordini di cambiamento, le Questioni e le attività del flusso di lavoro, selezionare la scheda Assegnazione automatica e la casella di controllo Assegnazione automatica abilitata nelle pagine Dettagli categoria Cambiamento, Dettagli categoria Questione e Dettagli del modello flusso di lavoro CA Technologies.

Nota: fare clic su Modifica per visualizzare la casella di controllo Assegnazione automatica abilitata.

Esempio: abilitazione dell'assegnazione automatica per un'area richiesta/incidente/problema

In questo esempio viene mostrato come abilitare l'assegnazione automatica per un'area richiesta/incidente/problema.

1. Nella scheda Amministrazione, accedere a Service Desk, Richieste/Incidenti/Problemi, Aree.

   Viene visualizzata la pagina Elenco Aree Richiesta/Incidente/Problema.

2. Fare clic sull'area per la quale si desidera configurare l'assegnazione automatica.

   Viene visualizzata la pagina Dettagli area Richiesta/Incidente/Problema.

3. Fare clic su Modifica.

   Viene visualizzata la pagina Aggiorna area Richiesta/Incidente/Problema.

4. Selezionare la scheda Assegnazione automatica e compilare i campi come indicato di seguito:

   Modalità assegnazione automatica

   Specifica come avviene l'assegnazione automatica. Utilizzare l'opzione Elemento della configurazione basato su per basare l'assegnazione automatica sul valore Attributo dell'elemento della configurazione assegnabile.

   - **Disabilitata**—Basa l'assegnazione automatica sull'opzione Impostazione predefinite dell'area al momento dell'installazione.
   - **Basata sull'elemento della configurazione** —Basa l'assegnazione automatica sul valore dell'Attributo dell'elemento della configurazione assegnabile.
   - **Basata sulla posizione** —Basa l'assegnazione automatica sul valore della posizione.

   Attributo dell'elemento della configurazione assegnabile

   Specifica l'attributo dell'elemento della configurazione da utilizzare per l'assegnazione al gruppo. È possibile immettere direttamente un valore o fare clic sulla lente d'ingrandimento per cercare un attributo.

5. Fare clic su Salva.

   L'area richiesta/incidente/problema è abilitata per l'uso dei valori predefiniti inseriti automaticamente nei ticket richiesta, incidente o problema assegnati all'area.

Sostituzione dell'assegnazione automatica

Utilizzare l'opzione di sostituzione dell'assegnazione automatica (autoasg_override) in Gestione opzioni per determinare se la funzione Assegnazione automatica deve sostituire un analista o un gruppo che è stato impostato durante la creazione di un ticket.

È possibile che altre funzioni di CA SDM abbiano impostato l'assegnatario e/o il gruppo prima che Assegnazione automatica venisse attivata. È possibile personalizzare il sistema impostando questa opzione su uno dei valori riportati di seguito:

0

Include l'assegnatario e/o il gruppo esistente. L'assegnazione automatica non viene effettuata se l'assegnatario e/o il gruppo è stato impostato durante la creazione del ticket.

1

Ignora l'assegnatario e/o il gruppo esistente. L'assegnazione automatica prosegue e tenta di trovare un assegnatario e/o un gruppo.

È possibile impostare l'Assegnatario e/o il Gruppo in vari modi:

- Manualmente mediante l'analista
- Opzioni di impostazione dell'assegnatario e impostazioni predefinite dell'area
- Modelli richiesta
- Integrazione di CA NSM

Nota: se si disinstalla l'opzione di sostituzione dell'assegnazione automatica, viene ripristinata la modalità predefinita (0).

Controlli di assegnazione

Sono disponibili opzioni e controlli per configurare l'assegnazione automatica. Le funzioni di CA SDM possono influenzare i campi Assegnatario e/o Gruppo di un ticket prima che il processo di assegnazione automatica abbia luogo. Si consiglia di controllare i controlli di assegnazione prima di implementare l'assegnazione automatica.

Assegnazione manuale

L'analista può selezionare manualmente l'assegnatario e/o il gruppo durante la creazione di un ticket.

Opzione Assignee_set

Per impostazione predefinita, CA SDM imposta automaticamente l'utente collegato come assegnatario della richiesta se l'utente in questione è un analista. L'opzione Assignee_set di Gestione opzioni consente di controllare questo comportamento. Solitamente, questa opzione viene installata per impostazione predefinita.

Iss assignee_set

L'opzione Iss assignee_set imposta automaticamente l'utente collegato come assegnatario della questione, se l'utente in questione è un analista. Questa funzione è analoga ad Assignee_set, ma viene utilizzata per le questioni anziché per le richieste.

Area_Defaults

Questa opzione consente di impostare le operazioni eseguite quando si specifica l'area richiesta nella pagina di dettagli di una richiesta. Questa opzione consente di impostare l'assegnatario e il gruppo ogni volta che l'area richiesta cambia. Vengono utilizzati l'assegnatario e il gruppo predefiniti dell'area richiesta e il processo ha luogo prima dell'assegnazione automatica.

Questa opzione viene installata per impostazione predefinita.

Nota: l'opzione Category_Defaults fornisce funzionalità simili per gli ordini di cambiamento. L'opzione Iss_Category_Defaults fornisce funzionalità simili per le questioni.

Opzioni richiesta per assegnatari e gruppi

In Gestione opzioni sono disponibili diverse opzioni per il controllo della creazione dei ticket non assegnati. L'ambito è comune a tutte queste opzioni. Queste opzioni influenzano la creazione di tutti i tipi di ticket indicati, indipendentemente dal fatto che la funzione Assegnazione automatica sia attiva. Se la condizione indicata non viene soddisfatta, non è possibile salvare il ticket nuovo o aggiornato.

Le seguenti opzioni controllano la creazione dei ticket senza la specifica di un assegnatario:

require_change_assignee

Applicazione: Gestione ordini di cambiamento

Descrizione: rende obbligatorio il campo Assegnatario di un ticket ordine di cambiamento

require_issue_assignee

Applicazione: Gestione Questione

Descrizione: rende obbligatorio il campo Assegnatario di un ticket questione

require_incident_assignee

Applicazione: Gestione Richiesta

Descrizione: rende obbligatorio il campo Assegnatario di un ticket incidente

require_problem_assignee

Applicazione: Gestione Richiesta

Descrizione: rende obbligatorio il campo Assegnatario di un ticket problema

require_request_assignee

Applicazione: Gestione Richiesta

Descrizione: rende obbligatorio il campo Assegnatario di un ticket richiesta

Le seguenti opzioni controllano la creazione dei ticket senza la specifica di un gruppo:

require_change_group

Applicazione: Gestione ordini di cambiamento

Descrizione: rende obbligatorio il campo Gruppo di un ticket ordine di cambiamento

require_issue_group

Applicazione: Gestione Questione

Descrizione: rende obbligatorio il campo Gruppo di un ticket questione

require_incident_group

Applicazione: Gestione Richiesta

Descrizione: rende obbligatorio il campo Gruppo di un ticket incidente

require_request_group

Applicazione: Gestione Richiesta

Descrizione: rende obbligatorio il campo Gruppo di un ticket richiesta

require_problem_group

Applicazione: Gestione Richiesta

Descrizione: rende obbligatorio il campo Gruppo di un ticket problema

Modelli

È possibile utilizzare i modelli per impostare i valori in una nuova richiesta, in un nuovo ordine di cambiamento oppure in una nuova questione. Quelli relativi agli assegnatari e ai gruppi sono i campi maggiormente influenzati dai modelli.

Interfaccia di CA Network and Systems Management

Quando CA NSM e CA SDM vengono integrati e si creano le richieste da eventi di CA NSM, il parametro user_parms nelle definizioni delle regole dei writer viene passato all'interfaccia API testo. Il processo del writer di CA SDM (tngwriter) definisce i relativi parametri di sostituzione per la modifica del testo prima dell'invio all'interfaccia API testo. La parola chiave LOG_AGENT viene aggiunta in fondo all'input per impostare log_agent per la richiesta.

Nota: occorre aggiornare il fileText_API.cfg per tutti i campi aggiuntivi che vengono passati da Alert Management Systems CA NSM a CA SDM. Questo file è utilizzato per integrazioni con servizi Web, posta elettronica e AHD.DLL.

Ulteriori informazioni:

Parole chiave (a pagina 556)

Registro attività

La funzione Assegnazione automatica registra le informazioni come eventi nel registro attività di un ticket. Vengono registrate le informazioni sull'esito dell'assegnazione automatica e su eventuali condizioni anomale che potrebbero essersi verificate durante il processo.

Abilitazione della registrazione delle attività per gli attributi aggiuntivi

I registri delle attività visualizzano i valori di attributo dei Cambiamenti di oggetti. Gli oggetti, quali tutti i tipi di ticket, le attività del flusso di lavoro classiche, le indagini, i contatti e gli elementi della configurazione dispongono della funzionalità di registrazione dell'attività. È possibile abilitare la registrazione delle attività per gli attributi aggiuntivi in WSP.

Nota: è possibile visualizzare gli attributi semplici del registro attività, inclusi stringhe, numeri interi, data, durata e tipi SREL. Non è possibile visualizzare i registri delle attività per i tipi di elenco, ad esempio QRELs e BRELs.

Procedere come descritto di seguito:

1. Aprire WSP e inizio la progettazione schema.
2. Selezionare la tabella che si desidera modificare e aggiungere gli attributi aggiuntivi.
3. Per ciascun attributo, aggiungere +AUDITLOG() al campo UI_INFO definito a livello di sito.

   Importante. Se si aggiunge il flag AUDITLOG, *rimuovere* la funzione val_fieldupdate_site() per evitare la duplicazione dei registri attività.
4. Salvare e pubblicare lo schema.
5. Aprire nuovamente WSP e aggiungere i nuovi attributi ai moduli dei dettagli appropriati.
6. Aprire CA SDM e definire una associazione attività per gli attributi aggiuntivi.
7. Verificare le modifiche apportate.

   Ad esempio, aprire un'istanza dell'oggetto salvata precedentemente e modificare gli attributi interessati per verificare che vengano visualizzati i registri attività appropriati

Tracciamento dell'assegnazione automatica

In un'implementazione complessa della funzione Assegnazione automatica, è possibile che la funzione non prenda le decisioni previste. È possibile abilitare la funzione di traccia per comprendere meglio il flusso del processo. La funzione di traccia è solitamente disattivata. Quando viene attivata, vengono scritti numerosi messaggi nei file stdlog nella directory $NX_ROOT\log. I messaggi descrivono le varie decisioni prese dalla funzione Assegnazione automatica.

Prestare attenzione quando si implementa la funzione in un'installazione con volumi molto elevati, poiché il numero di messaggi che vengono generati potrebbe comportare un aumento eccessivo delle dimensioni dei file di registro. Nei sistemi con intensa attività, si potrebbe notare un peggioramento delle prestazioni. La funzione di traccia viene controllata dall'utilità pdm_logstat. I parametri di questa utilità rispettano l'uso delle maiuscole e delle minuscole. Assicurarsi di rispettare la sintassi dei parametri, come mostrato di seguito.

Per attivare la funzione di traccia, eseguire il comando seguente su ciascun server di CA SDM:

```
pdm_logstat –f auto.pm milestone
```

Per disattivare la funzione di traccia, eseguire il comando seguente su ciascun server di CA SDM:

```
pdm_logstat –f auto.pm
```

Query memorizzate

Per il controllo della disponibilità degli analisti, vengono fornite due query memorizzate. I manager di CA SDM possono aggiungerle al proprio contatore:

- **Analisti disponibili**: analisti contrassegnati come disponibili per l'assegnazione automatica
- **Analisti non disponibili**: analisti contrassegnati come non disponibili per l'assegnazione automatica

Modalità di assegnazione automatica dei ticket

L'assegnazione automatica precede l'assegnazione dei ticket come riportato di seguito:

1. L'operazione di salvataggio iniziale di un nuovo ticket richiama l'assegnazione automatica.

   Se una categoria o un'area non è configurata per l'assegnazione automatica, l'operazione si interrompe.

2. L'assegnazione automatica determina se Autoasg_override è installata.

   Se non è installata e al ticket è associato un assegnatario o un gruppo, l'elaborazione si interrompe.

3. Se i turni di lavoro sono correlati al ticket, viene valutata la data di apertura per determinare se un turno include il ticket.

   Se un turno non include il ticket, l'elaborazione si interrompe e l'assegnazione automatica tenta di accedere al gruppo e all'assegnatario predefiniti.

4. L'assegnazione automatica determina se i gruppi sono correlati al ticket.

   Se non si verificano corrispondenze, l'elaborazione si interrompe e l'assegnazione automatica tenta di assegnare il gruppo e l'assegnatario predefiniti.

5. L'assegnazione automatica esclude i gruppi cui è associato un turno di lavoro, in cui la data di apertura non rientra nell'intervallo di tempo del turno. I gruppi a cui non sono associati turni non vengono esclusi.

6. Di seguito viene illustrato cosa accade alle posizioni correlate al ticket.

   - Se il ticket è una richiesta e presenta un elemento della configurazione

     La posizione dell'elemento della configurazione viene confrontata con le posizioni correlate all'area Richiesta. Se non si verificano corrispondenze, l'elaborazione si interrompe e l'assegnazione automatica tenta di assegnare il gruppo e l'assegnatario predefiniti. In caso contrario, la posizione del cliente viene confrontata con le posizioni correlate all'area o alla categoria. Se non si verificano corrispondenze, l'elaborazione si interrompe e l'assegnazione automatica tenta di assegnare il gruppo e l'assegnatario predefiniti.

   - Se le posizioni sono associate all'area Richiesta o alla categoria

     Se le posizioni sono associate all'area Richiesta e l'elemento della configurazione (durante il processo di assegnazione automatica della Richiesta) o il cliente non presenta una posizione, la funzione Assegnazione automatica interrompe l'elaborazione.

7. La funzione Assegnazione automatica esclude i gruppi idonei con posizioni che non corrispondono alla posizione dell'elemento della configurazione (solo per le richieste) o del cliente. Se non rimangono gruppi, l'elaborazione si interrompe e l'assegnazione automatica tenta di assegnare il gruppo e l'assegnatario predefiniti.

8. La funzione Assegnazione automatica crea un elenco di analisti da ciascuno dei gruppi idonei rimanenti.

9. Gli analisti non disponibili vengono esclusi.

10. Vengono controllate le pianificazioni di lavoro degli analisti rimanenti. Gli analisti con pianificazioni di lavoro la cui data di apertura non rientri nelle relative pianificazioni vengono esclusi.

11. Se non rimangono analisti, l'elaborazione si interrompe e l'assegnazione automatica tenta di assegnare il gruppo e l'assegnatario predefiniti.

12. Tutti gli altri analisti rimanenti vengono classificati in base al numero di ticket attivi assegnati.

13. Il ticket viene assegnato all'analista e al gruppo associato con il minor numero di ticket attivi. In situazioni di parità, viene scelto il primo analista del gruppo.

Avvio assegnazione automatica
Il flag sostituzione è impostato?
Sì
No
Esiste già un assegnatario?
Sì
Registrazione messaggio di errore "AHD05441 Al ticket è assegnato un assegnatario"
Esci
No
Esiste già un gruppo assegnato?
Sì
Registrazione messaggio di errore "AHD05442 Al ticket è assegnato un gruppo"
Esci
No
L'area richiesta/categoria è vuota?
Sì
Esci
No
I turni sono associati?
No
Sì
La data di apertura rientra in uno dei turni?
No
Registrazione messaggio di errore "AHD 05443 Mancata assistenza durante questo periodo"
Assegnare l'assegnatario e il gruppo predefiniti dell'area richiesta
Esci
Sì
Passare a pagina 2
PAGINA
1 di 4

Segue da pagina 1
I gruppi sono ssociati?
No
Registrazione messaggio di errore
"AHD 05444 Nessun gruppo di assistenza per questo ticket"
Assegnare l'assegnatario e il gruppo predefiniti dell'area richiesta
Esci
Sì
Trovare tutti i gruppi associati a questa area richiesta/categoria
Filtrare i gruppi con turni associati che non soddisfano la data di apertura del ticket
Elenco dei gruppi idonei
Le posizioni sono associate?
No
Passare a pagina 4
Sì
Trovare tutte le posizioni associate
Passare a pagina 3
PAGINA
2 DI 4

Segue da pagina 2
Sì
No
Questa è una richiesta ed esiste un asset?
No
L'asset ha una posizione?
Sì
Sì
Il cliente ha una posizione?
No
Registrazione messaggio di errore
"AHD05450 L'area richiesta presenta delle posizioni, ma la risorsa interessata no"
Sì
La posizione dell'asset è supportata da questa area richiesta?
No
La posizione del cliente è supportata da questa area richiesta/ categoria?
Sì
No
Registrazione messaggio di errore
"AHD05448 L'Area richiesta/categoria presenta delle posizioni, ma l'utente finale Interessato no"
Registrazione messaggio di errore
"AHD05449 Nessuna posizione idonea dell'area richiesta che supporta la posizione della risorsa interessata"
Registrazione messaggio di errore
"AHD05447 Nessuna posizione idonea dell'area richiesta/ categoria che supporta la posizione dell'utente finale interessato"
Assegnare l'assegnatario e il gruppo predefinit dell'area richiesta
Assegnare l'assegnatario e il gruppo predefiniti dell'area richiesta
Esci
Esci
Assegnare l'assegnatario e il gruppo predefiniti dell'area richiesta
Assegnare l'assegnatario e il gruppo predefiniti dell'area richiesta
Esci
Esci
Elenco dei gruppi idonei
Filtrare i gruppi che non supportano la posizione dell'asset o del cliente
Passare a pagina 4
PAGINA
3 DI 4

Segue da pagina 2
Segue da pagina 3
Nell'elenco sono rimasti gruppi idonei?
No
Sì
Registrazione messaggio di errore
"AHD05452 Impossibile trovare un gruppo idoneo per supportare questo ticket"
Ottenere un elenco degli analisti dai gruppi idonei
Assegnare l'assegnatario e il gruppo predefiniti dell'area richiesta
Filtrare gli analisti con turni pianificati che non soddisfano la data di aperta della richiesta
Esci
Ci sono analisti disponibili?
No
Sì
Assegnare l'analista/gruppo con il carico di lavoro minimo
Registrazione messaggio di errore
"AHD05453 Impossibile trovare un analista disponibile"
Invocare Auto_site.pm per accettare la selezione
Assegnare l'assegnatario e il gruppo predefiniti dell'area richiesta
Esci
Messaggio
analista/gruppo assegnato
Esci
PAGINA
4 DI 4

Assegnazione automatica delle attività flusso di lavoro

L'assegnazione automatica utilizza la logica di elaborazione per assegnare le attività flusso di lavoro come segue:

1. La funzione Assegnazione automatica viene richiamata quando un'attività del flusso di lavoro passa allo stato In sospeso. Se il modello flusso di lavoro utilizzato per creare l'attività non è abilitato per l'assegnazione automatica, l'elaborazione si interrompe. Se la categoria ordine di cambiamento o questione padre non è abilitata per l'assegnazione automatica, l'elaborazione si interrompe.
2. La funzione Assegnazione automatica verifica se l'opzione Autoasg_override è installata. Se non è installata e all'attività è associata un assegnatario o un gruppo, l'elaborazione si interrompe.
3. Viene verificata la presenza di contatti associati al modello flusso di lavoro utilizzato per creare l'attività. Se non ci sono contatti, l'elaborazione si interrompe.
4. La funzione Assegnazione automatica genera un elenco di tutti i contatti che sono membri dei gruppi attualmente associati al modello flusso di lavoro con il quale è stata creata l'attività. Tutti i contatti dell'elenco membri di gruppi vengono eliminati.
5. Tutti i contatti rimanenti vengono classificati in base al numero di attività di tipo ordine di cambiamento o questione attive assegnate.
6. L'attività viene assegnata al contatto e al gruppo associato con il minor numero di attività attive.

Avvio assegnazione automatica
Il modello è attivato?
No
Assegnare l'assegnatario e il gruppo predefiniti del modello
Esci
Sì
La categoria padre è attivata?
No
Assegnare l'assegnatario e il gruppo predefiniti del modello
Esci
Sì
Il flag sostituzione è impostato?
Sì
No
Esiste già un assegnatario?
Sì
Registrazione messaggio di errore "AHD05441 All'attività è assegnato un assegnatario"
Esci
No
Esiste già un gruppo assegnato?
Sì
Registrazione messaggio di errore "AHD05442 All'attività è assegnato un gruppo"
Esci
No
Passare a pagina 2
PAGINA
1 DI 2

Segue da pagina 1
I gruppi sono associati?
No
Registrazione messaggio di errore
"AHD05444 Nessun gruppo di assistenza per questa attività"
Assegnare l'assegnatario e il gruppo predefiniti del modello
Esci
Sì
Ottenere tutti i contatti dai gruppi associati al modello
Filtrare i contatti che sono gruppi
Elenco degli assegnatari idonei
Assegnare l'analista/gruppo con il carico di lavoro minimo
Invocare Auto_site.pm per accettare la selezione
Messaggio del registro
Analista/gruppo assegnato
Esci
PAGINA
2 DI 2

Assegnazioni automatiche basate sull'elemento della configurazione

Le assegnazioni automatiche basate sull'elemento della configurazione consentono di creare assegnazioni a gruppi specifici applicabili a scenari specifici. È possibile specificare che per ticket di richiesta/incidente/problema aperti per un'area particolare, il valore di un attributo dell'elemento della configurazione associato con il ticket ne controlli l'assegnazione.

Assegnazioni basate sull'elemento della configurazione e assegnazioni automatiche basate sulla località rappresentano opzioni esclusive perché è possibile selezionare un solo algoritmo da utilizzare in un'area Richiesta/Incidente/Problema. Assegnazioni basate su elementi della configurazione e assegnazioni automatiche basate sulla località servono entrambe per assegnare ticket al momento della loro creazione. Tuttavia, le assegnazioni automatiche basate sull'elemento della configurazione si distinguono dalle altre perché riassegnano anche i ticket ogni volta che viene modificata l'area Richiesta/Incidente/Problema di un ticket o di un elemento della configurazione.

Esempio: area Richiesta/Incidente/Problema assegna ticket a un gruppo

Quando si configura l'area Rete (per Richieste/Incidenti/Problemi) per eseguire assegnazioni automatiche basate sull'elemento della configurazione utilizzando l'attributo network_contact_uuid (Operazioni di rete) come valore Attributo dell'elemento della configurazione assegnabile, eventuali ticket aperti per l'area Rete vengono assegnati automaticamente al gruppo specificato nel campo Operazioni di rete dell'elemento della configurazione associato al ticket. Se al ticket non è associato alcun elemento della configurazione oppure se il valore del campo Operazioni di rete dell'elemento della configurazione è vuoto o non specifica un gruppo, l'assegnazione non viene effettuata. In questi casi, il sistema agisce conformemente all'opzione Gestione opzioni, Impostazioni predefinite area e assegna il ticket utilizzando i campi Gruppo e Assegnatario della categoria.

Modalità di funzionamento dell'assegnazione automatica basata su elementi della configurazione

I ticket richiesta/incidente/problema devono specificare quanto riportato di seguito affinché venga eseguita l'assegnazione automatica basata su elementi della configurazione:

- Un elemento della configurazione e un'area
- L'area deve avere l'opzione Assegnazione automatica impostata su Elemento della configurazione basato su.

Quando un analista crea e assegna un ticket a tale area o modifica l'area su un ticket esistente, viene esaminato il campo Attributo dell'elemento della configurazione assegnabile dell'area. Il valore del campo Attributo dell'elemento della configurazione assegnabile viene utilizzato come nome di attributo e il programma cerca quindi di trovare un attributo con nome identico nell'elemento della configurazione associato al ticket. Se l'attributo nell'elemento della configurazione include un gruppo, il ticket viene assegnato a tale gruppo.

Il diagramma riportato di seguito illustra in maggior dettaglio il processo di assegnazione automatica basata sull'elemento della configurazione:

1. CA SDM verifica quanto segue:
   a. L'opzione autoasg_override è impostata?
   b. Il ticket specifica un'area con assegnazione automatica auto_assign_mode=2?
   c. La categoria specifica un attributo dell'elemento della configurazione assegnabile?
   d. Il ticket specifica un elemento della configurazione?
   e. L'elemento della configurazione ha un valore dell'attributo dell'elemento della configurazione assegnabile?
   f. Il valore specifica un gruppo nell'attributo dell'elemento della configurazione?
   g. L'assegnatario del ticket è un membro del gruppo del ticket?

2. Se le risposte a tutte le domande precedenti sono positive, CA SDM imposta l'attributo gruppo del ticket sull'attributo gruppo dell'elemento della configurazione e registra l'assegnazione nel registro attività.

   Nota: il diagramma seguente mostra come l'assegnazione automatica basata sull'elemento della configurazione utilizzi la variabile NX_CHECK_ASSIGNEE_IN_AREA_DEFAULTS per stabilire se l'opzione Area è attivata. NX_CHECK_ASSIGNEE_IN_AREA_DEFAULTS è una variabile del file NX.env, che si trova nella directory $NX_ROOT\.

3. Il ticket viene assegnato al gruppo.

Avvio processo
autoasg_override impostato?
No
Attr. di gruppo del ticket impostato?
Sì
Il ticket indica una cat. con auto_assign_mode = 2?
No
Sì
La cat. indica un attr. dell'elem. config. assegnabile?
Cat. reg/assegnaz. elem.config. Ignorata nel reg.attività
No
Sì
Il ticket specifica un elem.config.?
No
Opzione Area_Defaults installata e abilitata?
Sì
No
Sì
Impost.attributo di gruppo ticket sul valore di gruppo di cat.
Valore specificato per elem. config. assegnabile?
Opzione NX_CHECK_ASSIGN_EE_IN_AREA_DEFAULT abilitata?
No
Sì
Sì
Il valore elem. config. assegnabile indica un gruppo?
Assegnatario cat. Membro del gruppo di cat.?
Sì
Assegnatario cat. Membro del gruppo di cat.?
Sì
Impost. attr.di gruppo per attr.dell'elem.config.
No
No
No
Assegnatario ticket membro del gruppo?
Sì
Registrare assegnazione in reg.attività
No
No
No
Cancellare attributo assegnatario ticket
Attr.assegnatario richiesto?
Sì
Annullare salvataggio operazione
Processo completato

Ulteriori informazioni:

Sostituzione dell'assegnazione automatica (a pagina 492)

Attivazione delle assegnazioni automatiche basate sull'elemento della configurazione

Le assegnazioni automatiche basate sull'elemento della configurazione consentono di creare assegnazioni a gruppi specifici applicabili a scenari specifici. È possibile specificare che per ticket di richiesta/incidente/problema aperti per un'area particolare, il valore di un attributo dell'elemento della configurazione associato con il ticket ne controlli l'assegnazione. L'assegnazione automatica basata sull'elemento della configurazione riassegna ticket ogni volta che cambia l'area Richiesta/Incidente/Problema di un ticket o di un elemento della configurazione.

Nota: l'opzione autoasg_override di Gestione opzioni controlla le circostanze in cui viene eseguita l'assegnazione automatica. Quando si imposta questa opzione su 1, l'eventuale assegnatario e le impostazioni del gruppo vengono ignorate e i ticket vengono assegnati automaticamente in tutti i casi. Se si desidera che l'assegnazione automatica di ticket venga utilizzata in CA SDM solo quando i ticket non sono già stati assegnati, impostare il valore su 0.

Per attivare l'assegnazione automatica basate sull'elemento della configurazione

1. Nella scheda Amministrazione, accedere a Service Desk, Richieste/Incidenti/Problemi, Aree.

   Viene visualizzato l'Elenco aree richiesta/incidente/problema.

2. Selezionare l'area da modificare.

   Viene visualizzata la pagina Dettagli area.

3. Fare clic su Modifica.

   Viene visualizzata la pagina Update Area.

4. Selezionare la scheda Assegnazione automatica e compilare i campi come indicato di seguito:

   Modalità assegnazione automatica

   Specifica come avviene l'assegnazione automatica. Utilizzare l'opzione Elemento della configurazione basato su per basare l'assegnazione automatica sul valore Attributo dell'elemento della configurazione assegnabile.

Attributo dell'elemento della configurazione assegnabile

Specifica l'attributo dell'elemento della configurazione da utilizzare per l'assegnazione al gruppo. È possibile immettere direttamente un valore o fare clic sulla lente d'ingrandimento per cercare un attributo.

Fare clic su Salva.

L'assegnazione automatica viene attivata. Le assegnazioni automatiche basate sull'elemento della configurazione vengono eseguite utilizzando l'attributo specificato nel campo Attributo dell'elemento della configurazione assegnabile.

Capitolo 13: Gestione del database

Questa sezione contiene i seguenti argomenti:

Utilità di gestione del database (a pagina 515)
Selezione e configurazione del database (a pagina 515)
Utilità di caricamento del database (a pagina 516)
Backup del database (a pagina 519)
Ripristino del database (a pagina 519)
Sostituzione delle tabelle del database (a pagina 519)
Annullamento dei riferimenti dati (a pagina 521)
Miglioramento delle prestazioni con la cache del browser (a pagina 536)
Modifica del file di configurazione (a pagina 538)

Utilità di gestione del database

È possibile eseguire utilità per la gestione del database mentre CA SDM è spento. Se si eseguono le utilità di gestione del database e si utilizza un database diverso dal repository predefinito di CA SDM, è necessario impostare le variabili di ambiente per il database.

Nota: per informazioni sull'impostazione delle variabili di ambiente, consultare la documentazione relativa al database in uso.

Selezione e configurazione del database

È possibile selezionare il database e configurarlo per l'utilizzo con CA SDM.

Per selezionare e configurare un database

1. Selezionare il database dall'elenco a discesa Tipo database, quindi fare clic su Avanti.

   Viene visualizzata la pagina di configurazione del database selezionato.

2. Inserire le informazioni sul database nella pagina di configurazione del database, quindi fare clic su Avanti.

   La configurazione del database è stata completata.

   Nota: usare il pulsante ? di questa pagina per ottenere informazioni sulla configurazione dei campi del database selezionato.

Nelle pagine di configurazione vengono visualizzati i pulsanti seguenti.

?

Consente di visualizzare gli argomenti della Guida per la pagina corrente.

Annulla

Consente di annullare le impostazioni di configurazione specificate nella sessione corrente.

Indietro

Consente di tornare alla pagina precedente senza salvare le modifiche apportate nella pagina corrente.

Successivo

Consente di passare alla pagina successiva dopo aver salvato tutte le modifiche apportate nella pagina corrente.

Utilità di caricamento del database

L'utilità di caricamento del database, pdm_userload, aggiunge, aggiorna e seleziona i record di database di CA SDM. È necessario creare un file di input in formato ASCII formattato per l'utilità pdm_userload e selezionare le tabelle da caricare e i campi opzionali da aggiungere.

Importante: L'utilità pdm_userload accede al database di CA SDM e non interagisce direttamente con i processi dei software applicativi. Le voci di inventario aggiunte al database con l'utilità pdm_userload non aggiornano l'assistente e/o gli elenchi di selezione fin quando l'applicazione non viene arrestata e riavviata.

Sebbene sia possibile eseguire l'utilità pdm_userload con l'applicazione attiva, le prestazioni del sistema ne risentiranno negativamente. Per ottenere risultati ottimali, assicurarsi che il server in background sia in esecuzione e che nessun utente utilizzi l'interfaccia client prima dell'esecuzione dell'utilità pdm_userload.

Nota: Per aggiungere record contenenti campi con riferimenti-incrociati, utilizzare l'utilità pdm_deref.

Ulteriori informazioni:

Annullamento dei riferimenti dati (a pagina 521)

Modalità di creazione e utilizzo di un file di input

È possibile utilizzare un file di input e l'utilità pdm_userload per inserire dati nelle tabelle del database.

Il formato del file di input è il seguente:

- Racchiudere i valori dei campi tra virgolette (“valore”) e separare i valori con una virgola e uno spazio (“valore1”, “valore2”).
- per includere le virgolette nelle stringhe di testo, farle precedere da una barra rovesciata (\). Per impostare un campo data/ora sulla data e ora correnti, utilizzare il parametro @NOW@ per il valore di input.
- Racchiudere ogni record tra parentesi graffe separate da spazi, come segue:

  ```
  ( { valori campi record } )
  ```

- Se si applica una sintassi appropriata, i record di input possono essere distribuiti su più righe nel file di input; tuttavia, i singoli campi devono essere scritti interamente su un'unica riga. Per i campi che devono essere distribuiti su più righe, ad esempio i commenti, i valori possono includere un carattere di nuova riga (\n) al fine di forzare una nuova riga quando il campo del database viene visualizzato.
- I caratteri di nuova riga sono richiesti in modo esplicito solo nei casi in cui è necessaria una speciale formattazione. Il testo normale viene automaticamente visualizzato con le interruzioni di riga appropriate, come mostrato nell'esempio seguente:

  ```
  "Stato record \"COMPLETO\""
  ```

Per creare un file di input per l'utilità pdm_userload, attenersi alla procedura seguente:

1. Determinare la tabella da caricare e i campi della tabella in cui inserire i dati.

   Per ogni record caricato, è necessario inserire i dati nei campi chiave Nome o Simbolo.

2. Creare una copia del file *nomefile*.dat appropriato per la tabella che si sta caricando.
3. Modificare la nuova copia creata del file *nomefile*.dat, come indicato di seguito:
   a. Aggiungere una voce per ogni record da caricare.
   b. A partire dalla riga successiva alla riga TABLE (vedere l'esempio seguente), eliminare i campi in cui non si intende inserire i dati.

      ```
      TABLE nome_tabella
      nomecampo1 nomecampo4 . . nomecampoN
      ```

4. Salvare il file e uscire dall'editor.
5. Eseguire l'utilità pdm_userload e specificare il file, come mostrato nell'esempio seguente. In questo esempio, il nome del file di input è myData.dat:

   ```
   pdm_userload -f myData.dat
   ```

   I dati vengono inseriti nella tabella del database.

Ulteriori informazioni:

pdm_userload - Aggiunta, aggiornamento ed eliminazione dei record del database (a pagina 1166)

Eliminazione e ripristino dei vincoli

Alcune tabelle mdb il cui nome inizia con ca_ (ad esempio ca_contact_) presentano vincoli di riferimento che possono creare problemi durante il caricamento di massa dei dati tramite gli strumenti pdm_load, pdm_userload e pdm_restore. Se è richiesto il caricamento di massa di queste tabelle, potrebbe essere necessario eliminare i vincoli di riferimento prima del caricamento dei dati.

Per eliminare e ripristinare i vincoli vengono forniti due script SQL per ciascun tipo di DBMS. Prima del caricamento di massa dei dati delle tabelle ca_*, eseguire la versione Drop dello script per l'eliminazione. Una volta completato il caricamento dei dati, eseguire la versione Add dello script per l'aggiunta.

Per SQL Server, gli script sono collocati nella directory *directory-installazione*\samples\views\SQLServer. Eseguire questo comando per eliminare i vincoli:

```
osql -E -e < SQLDropConstraints.sql'
```

Eseguire questo comando per aggiungere nuovamente i vincoli:

```
osql -E -e < SQLAddConstraints.sql
```

Per SQL Server, gli script sono collocati nella directory *directory-installazione*\samples\views\SQLServer.

Eseguire questo comando per eliminare i vincoli:

```
sqlplus mdbadmin/ <password> < OracleDropConstraints.sql
```

Eseguire questo comando per aggiungere nuovamente i vincoli:

```
sqlplus mdbadmin/ <password> < OracleAddConstraints.sql
```

Backup del database

È possibile eseguire il backup del contenuto di una singola tabella, di più tabelle o dell'intero database di CA SDM, utilizzando l'utilità di backup del database, pdm_backup. L'output dell'utilità di backup è un file in formato ASCII che può essere utilizzato dall'utilità pdm_restore.

Come parte del processo, l'utilità pdm_backup per prima cosa arresta i daemon (UNIX) o i servizi (Windows).

Ulteriori informazioni:

pdm_backup - Scrittura di tabelle di database in file ASCII (a pagina 1124)

Ripristino del database

L'utilità di ripristino del database, pdm_restore, consente di caricare un file di output generato dall'utilità pdm_backup nel database di CA SDM. Come prima cosa, l'utilità pdm_restore arresta i daemon (UNIX) o i servizi (Windows). Quindi ripristina, cancella e sostituisce tutti i record del database esistenti. Utilizzare il file in formato ASCII formattato creato dall'utilità pdm_backup come input per l'utilità pdm_restore.

È possibile utilizzare le utilità pdm_restore e pdm_userload anche per accedere all'applicazione CA SDM in caso di danneggiamento irreversibile del database. Se il livello di danneggiamento del database è tale da non consentire l'accesso all'applicazione e il problema non può essere risolto con nessun altro metodo, eseguire nuovamente la configurazione e reinizializzare il database per ricreare il database e inserire i dati di riferimento e le tabelle di sistema.

Questa procedura inizializza il database allo stesso modo in cui era stato inizializzato durante l'installazione originale. È ora possibile accedere a CA SDM. È possibile utilizzare l'utilità pdm_restore per ripristinare la copia di backup del database più recente.

Ulteriori informazioni:

pdm_restore - Ripristino di un database (a pagina 1157)

Sostituzione delle tabelle del database

L'utilità pdm_replace consente di sostituire in modo semplice e veloce l'intero contenuto di una tabella del database di CA SDM con nuove informazioni. Questa utilità risulta particolarmente utile per le revisioni intense delle tabelle di ricerca.-

Nota: l'utilità pdm_replace utilizza lo stesso formato di file di input dell'utilità pdm_userload. È possibile creare un file di input per l'utilità pdm_replace utilizzando l'utilità pdm_extract. Tuttavia, non è possibile utilizzare l'output generato dall'utilità pdm_backup come input per l'utilità pdm_replace.

Ulteriori informazioni:

pdm_replace - Sostituzione di una tabella di database (a pagina 1154)
Modalità di creazione e utilizzo di un file di input (a pagina 517)

Estrazione dei dati

L'utilità pdm_extract che consente di estrarre i dati dal database di CA SDM e produrre output in vari formati. È possibile elaborare ulteriormente questi dati oppure utilizzarli come input in altre applicazioni, ad esempio nei fogli di lavoro o in altri database.

Con l'utilità pdm_extract è possibile effettuare le seguenti operazioni:

- Eseguire il dump dell'intero database di CA SDM
- Eseguire il dump di una o più tabelle di database
- Estrarre informazioni specifiche dal database e generare l'output in uno dei tre formati seguenti:
  - Output compatibile con l'utilità pdm_userload
  - Output in formato CSV (Comma-Separated Value)
  - Output in stile report informale-

Ulteriori informazioni:

pdm_extract - Estrazione dei dati dal database (a pagina 1134)

Uso dell'utilità di estrazione dati in UNIX

Prima di utilizzare l'utilità di estrazione dati di CA SDM su UNIX, è necessario:

1. Impostare il valore della variabile di ambiente $NX_ROOT sul percorso completo della directory di installazione di CA SDM definita durante l'installazione.
2. Aggiungere $NX_ROOT/bin alla variabile di ambiente PATH.
3. Impostare il valore di umask su 000.

Selezione dei dati per l'estrazione

Per selezionare i dati da estrarre, l'utilità di estrazione dati utilizza un sottoinsieme di istruzioni SQL integrale con le regole seguenti:

- Le funzioni SQL seguenti sono supportate specificatamente nel sottoinsieme:
  - IS NULL, IS NOT NULL, LIKE
  - Istruzioni SELECT e clausole WHERE
- Le funzionalità SQL seguenti non sono supportate nel sottoinsieme:
  - Istruzioni di unione
  - Tabulazioni e caratteri di nuova-riga
  - Clausole diverse da SELECT, FROM e WHERE
  - Carattere asterisco (*) nelle istruzioni SELECT
  - Istruzioni SELECT nidificate
  - Funzioni aggregate
- Tutte le parole SQL riservate devono essere scritte in maiuscolo
- Ogni token in una clausola WHERE deve essere separato da uno spazio
- Tutte le specifiche di data/ora devono essere in uno dei tre formati seguenti:
  - Secondi trascorsi da 12:00:00 a.m. 1/1/1970 GMT (Greenwich Mean Time, ora di Greenwich):

    ```
    data_inizio< oppure >174182431500
    ```
  - Formato SQL DATE:

    ```
    data_inizio< oppure >DATE '2001-11-28'
    ```
  - Formato SQL TIMESTAMP:

    ```
    data_inizio< oppure >TIMESTAMP '2001-07-04 15:45:00'
    ```

Nota: il formato TIMESTAMP si basa sull'ora GMT. È possibile regolare i fusi orari aggiungendo o sottraendo i numeri di ore appropriati, ad esempio: 2001-03-23 14:00:00+02:00 o 2001-06-06 04:45:00-09:00.

Annullamento dei riferimenti dati

L'utilità pdm_deref è uno strumento per l'annullamento dei riferimenti che converte i dati provenienti da origini diverse in un formato adatto al caricamento nel database di CA SDM. L'annullamento dei riferimenti estrae gli ID interni per i campi con riferimenti incrociati.- È possibile avvalersi di questa utilità per il calcolo dei valori relativi all'inattività del sistema e degli SLA.

L'utilità pdm_deref converte i dati in uno dei seguenti formati:

- Output compatibile con l'utilità pdm_userload, adatto per il caricamento dei dati nel database di CA SDM
- Output in formato CSV (Comma-Separated Value)
- Output in stile report informale-

Ulteriori informazioni:

pdm_deref - Annullamento del riferimento (dati in formato ASCII) (a pagina 1128)

Esempio di utilizzo di pdm_deref

Il seguente esempio mostra come usare l'utilità pdm_deref in un sistema di tracciamento dei ticket CA SDM.

Si prenda come esempio un sistema di tracciamento dei ticket esistente implementato su un foglio di lavoro con le colonne Descrizione problema, Nome e cognome tecnico e Data immissione. Queste colonne corrispondono ai campi description, assignee e open_date della tabella Change_Request di CA SDM. Il campo Descrizione problema contiene lo stesso tipo di dati del campo description. Il campo assignee è un campo numerico, mentre il formato del campo corrispondente Nome e cognome tecnico nel foglio di lavoro è "cognome, nome".

Per utilizzare pdm_deref

1. Caricare i nomi dei tecnici nella tabella Contatto.
2. Preparare un file di input pdm_deref con le informazioni disponibili.
3. Creare un file di specifiche per associare i nuovi nomi dei contatti ai valori della colonna assignee.
4. Preparare un file di input pdm_userload da utilizzare per aggiornare la tabella Change_Request.

Questo processo viene descritto in dettaglio nei punti seguenti:

1. Preparare un file di input per l'utilità pdm_userload, location.dat, per la tabella Location, come indicato di seguito:

   ```
   TABLE ca.location
   location_name address_2 address_2
   {"Boulder NCC - NQ", "716 Main
       Street","Boulder, CO 84302"}
   {"Colorado Springs NCC", "2765 Spring Street",
       "Colorado Springs, CO 84303"}
   {"Denver NCC", "3765 Stoneridge Way", "Denver,
       CO 80254"}
   ```

2. Caricare i dati, come indicato di seguito:

   ```
   pdm_load -f location.dat
   ```

3. Preparare un file di input, contact.dat, con le informazioni originali, come indicato di seguito:

   ```
   TABLE ca.contact
   last_name first_name middle_name location pri_phone_number
   {"Harrison", "Frank," "Harold", "NCC - HQ", "303-555-2333"}
   {"Hertzog", "William", "I.", "Colorado Springs NCC", "303-966-1987"}
   {"Lyman", "Jeanie", "L.", "Denver NCC", "303-966-5301"}
   ```

4. Preparare un file di specifiche per lo strumento per annullare i riferimenti, contact.spec, come indicato di seguito:

   ```
   Deref
   {
   input = c_location
   output = location_uuid
   rule = "SELECT id FROM ca.location WHERE location_name=?"
   }
   ```

   Importante Non inserire spazi prima della parola chiave SELECT. L'utilità Deref utilizza il nome e il cognome dei contatti per ottenere i campi ID numerici appropriati per il caricamento della tabella Change_Request. Inoltre, gli "hook" rappresentati dai punti interrogativi (?), corrispondono ai campi di input specificati. È necessario che il numero di hook sia uguale a quello dei campi di input e che gli hook siano disposti nello stesso ordine.

5. Eseguire l'utilità pdm_deref, come indicato di seguito:

   ```
   pdm_deref -s contact.spec < contact.dat > contact.out
   ```

   Il contenuto del file di output, contact.out, è simile al seguente:

   ```
   TABLE ca.contact
   last_name first_name middle_name location.uuid pri_phone_number
   {"Harrison", "Frank", "Harold", "69499D5A2424884887E62EC9823F5E47",
   "303-555-2333"}
   {"Hertzog", "William", "I.", "86873FA40BA4234A8CF7A418D7C8B2DB",
   "303-966-1987"}
   {"Lyman", "Jeanie", "L.", "58AA42789957734E8BEE146D07F7AD49", "303-966-5301"}
   ```

6. Caricare il file contact.out nel database di CA SDM come indicato di seguito:

   ```
   pdm_load -i -f contact.out
   ```

   Nota: è necessario utilizzare il comando pdm_load al fine di specificare l'opzione –i.

7. (Solo in UNIX, facoltativo) Compilare uno script, Convert_Ticket, come nell'esempio indicato di seguito:

   ```
   #!/bin/sh
   pdm_load -i $1
   cat $2 | pdm_deref -s $3 | pdm_load -i
   ```

Eseguire quindi questo script, come indicato di seguito:

```
Convert Ticket location.dat contact.dat contact.spec
```

In questo esempio, per velocizzare il processo è stato utilizzato il comando pdm_load con il flag -i. Se si effettuano periodicamente questo tipo di aggiornamenti, eliminare il flag -i dal comando pdm_load, in modo che possa essere eseguito il controllo dei record duplicati.

Di seguito sono riportati altri esempi di file di specifiche per lo strumento per annullare i riferimenti:

```
Deref
{
        input = first_name, last_name, middle_name
        output = assignee
        rule = " SELECT id from ca.contact \

               WHERE first_name=? \
               AND last_name=? \
               AND middle_name=? "
}
```

Questa regola converte i tre campi first_name, last_name e middle_name con l'UUID del contatto appropriato. Se mancano tutti e tre i campi di input, la regola non viene applicata. La mancata corrispondenza genera un messaggio di errore, ma l'elaborazione continua. In caso di più corrispondenze, viene utilizzato il primo valore. Anche in questo caso, viene generato un messaggio di errore, ma l'elaborazione continua.

Uso della modalità dbadmin

La modalità dbadmin è un'utilità che avvia il livello di manipolazione dei dati del sistema CA SDM senza avviare il livello degli oggetti. Ciò consente di bloccare l'intero database per eseguire operazioni di gestione dei dati a basso livello senza compromettere l'integrità dei dati.

Si supponga, ad esempio, di dover utilizzare le utilità pdm_extract, pdm_load, pdm_deref e pdm_replace per effettuare operazioni di aggiornamento dei dati in batch sul sistema. Utilizzando la modalità dbadmin, l'amministratore applica sostanzialmente un blocco database sull'intero sistema. Entrambe le utilità di backup (pdm_backup) e di ripristino (pdm_restore) impostano automaticamente il sistema sulla modalità dbadmin per garantire operazioni di backup e ripristino coerenti.

La modalità dbadmin è particolarmente utile anche per personalizzare il sistema senza avviare il livello degli oggetti fin quando i dati non vengono modificati. Ad esempio, rendere "obbligatorio" un attributo in majic su un sistema esistente può confondere l'animatore se questo deve aggiornare un oggetto in cui il valore dell'attributo obbligatorio è Null. È possibile impostare il sistema sulla modalità dbadmin e aggiornare gli oggetti utilizzando l'utilità pdm_load, quindi avviare il sistema normalmente.

Per impostare la modalità dbadmin per il sistema

1. Arrestare CA SDM da Gestione servizi di Windows o eseguendo l'utilità pdm_halt dalla riga di comando.

   Nota: prima di arrestare il sistema, si consiglia di inviare un annuncio per avvisare gli utenti e per controllare se vi sono utenti collegati.

2. Dalla riga di comando, immettere il comando seguente rispettando le maiuscole e le minuscole:

   ```
   pdm_d_mgr –s DBADMIN
   ```

   Nota: non viene restituito alcun messaggio; tuttavia, ha luogo una breve pausa prima della restituzione del prompt dei comandi. Se la pausa non si verifica, controllare la sintassi del comando per verificare che i dati siano stati immessi correttamente.

3. Eseguire l'utilità pdm_status per verificare se il sistema è in modalità dbadmin.

   Nota: quando il sistema è in modalità dbadmin, restituisce il seguente stato, che indica che si può utilizzare il sistema in modo sicuro:

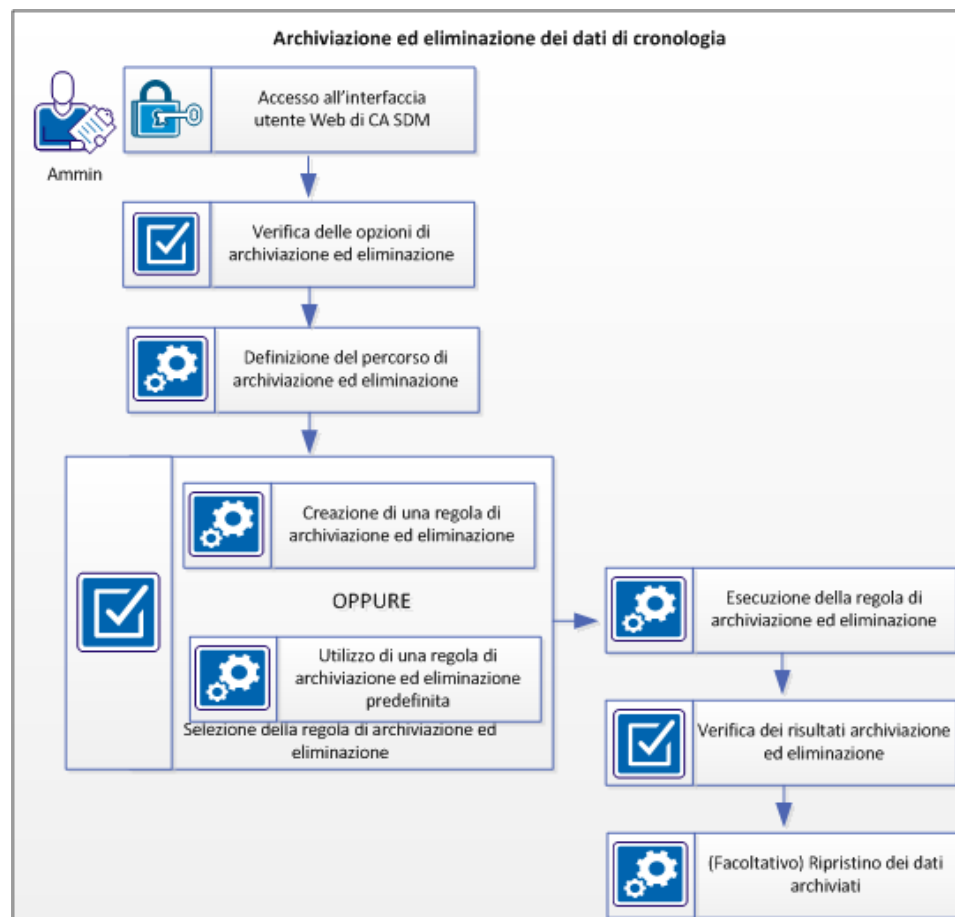
   ```
   C:\>pdm_status
   I daemon non sono in esecuzione.
   ```

4. Una volta completate le attività, eseguire l'utilità pdm_halt per arrestare la modalità dbadmin.

5. Riavviare il sistema seguendo le normali procedure.

Archiviazione ed eliminazione dei dati di cronologia

Rimuovere periodicamente i record della cronologia dal sistema affinché le dimensioni del database garantiscano prestazioni ottimali. Creare regole o attivare le regole predefinite per archiviare i record della cronologia ed eliminarli dal database.

Il diagramma seguente mostra la procedura per archiviare ed eliminare i dati della cronologia:

Procedere come descritto di seguito:

1. Aprire l'interfaccia utente Web di CA SDM (a pagina 191).
2. Verificare le opzioni di archiviazione ed eliminazione. (a pagina 527)
3. Definire il percorso di archiviazione ed eliminazione (a pagina 527).
4. Selezionare la regola di archiviazione ed eliminazione (a pagina 530).
   - Creare una regola di archiviazione ed eliminazione (a pagina 530).
   - Utilizzare una regola predefinita di archiviazione ed eliminazione (a pagina 533).

5. Eseguire la regola di archiviazione ed eliminazione.
6. Verificare i risultati di archiviazione ed eliminazione (a pagina 534).
7. (Se necessario) Ripristinare i dati archiviati (a pagina 535).

Apertura dell'interfaccia utente Web di CA SDM

Accedere all'interfaccia utente Web dai server seguenti, in base alla configurazione di CA SDM:

- Convenzionale: server primario o secondario
- Disponibilità avanzata: server applicazioni o in background

Verificare le opzioni di archiviazione ed eliminazione.

Prima di impostare la regola di archiviazione ed eliminazione, verificare le relative opzioni necessarie eventualmente per l'installazione o la disinstallazione, a seconda delle esigenze dell'organizzazione. Ad esempio, l'opzione default_schedule specifica la pianificazione predefinita (voce turno) utilizzata dalle regole di archiviazione ed eliminazione. Se il valore dell'opzione è impostato su un nome di voce turno non valido o su una stringa vuota, la regola non viene eseguita con il valore di pianificazione. Il campo Valore opzione determina la variabile NX_DEFAULT_SCHEDULE riportata nel file NX.env.

Selezionare Gestione opzioni, Archivia ed Elimina sulla scheda Amministrazione. Installare o disinstallare l'opzione richiesta.

Definizione del percorso di archiviazione ed eliminazione

È possibile definire la posizione in cui salvare i dati archiviati. Questo percorso può essere la directory principale di un server remoto o un percorso UNC. A seconda della configurazione di CA SDM, è necessario eseguire i server seguenti su Windows per accedere al percorso UNC:

- Convenzionale: server primario
- Disponibilità avanzata: server in background

Procedere come descritto di seguito:

1. Accedere all'interfaccia utente Web dai seguenti server di CA SDM, a seconda della configurazione di CA SDM:
    - Convenzionale: server primario o secondario
    - Disponibilità avanzata: server applicazioni o in background

2. Se si desidera archiviare ed eliminare gli allegati, completare i passaggi seguenti:

   a. Selezionare Libreria allegati, Repository nella scheda Amministrazione.

      Viene visualizzata la pagina Repository.

   b. Fare clic con il pulsante destro del mouse su un repository (ad esempio Service Desk) e selezionare Modifica.

      Viene visualizzata la pagina dei dettagli del repository.

   c. Modificare i seguenti campi:

      Tipo archivio

      Specifica l'azione di archiviazione ed eliminazione da eseguire sul contenuto del repository. Sono validi i seguenti valori:

      Nessuno: non vengono eseguiti processi di archiviazione ed eliminazione.

      Archivia ed elimina: i record della cronologia vengono scritti nel file specificato nel campo di archiviazione ed eliminati dal database.

      Elimina solamente: i record della cronologia vengono eliminati dal database, senza essere scritti nel file di archiviazione.

      Percorso archivio

      Specifica il percorso della directory o il percorso UNC in cui vengono spostati i file nel repository durante il processo di archiviazione.

      Credenziali UNC

      Specifica le credenziali per accedere al percorso UNC. Fare clic su Credenziali UNC per aprire la pagina Ricerca credenziali.

      - Se sono state già create le credenziali per accedere al percorso UNC specificato, usare i campi per cercare e selezionare le credenziali.
      - Se si desidera creare le credenziali, fare clic su Crea Nuovo. Per ulteriori informazioni sulla creazione di credenziali, consultare l'argomento Creazione di credenziali UNC (a pagina 463).

   d. Fare clic su Salva.

3. Se si desidera archiviare ed eliminare dati diversi dagli allegati, completare i passaggi seguenti:

   a. Nella scheda Amministrazione, selezionare Archivia ed elimina, quindi Impostazioni di archiviazione ed eliminazione.

   b. Immettere il percorso in cui si desidera memorizzare i dati archiviati ed eliminati nel campo Percorso regola di eliminazione e archiviazione.

   c. Se si utilizza un percorso UNC per memorizzare i dati archiviati, fare clic su Credenziali UNC.

Viene visualizzata la pagina Ricerca credenziali.

- Se sono state già create le credenziali per accedere al percorso UNC specificato, usare i campi per cercare e selezionare le credenziali UNC.
- Se si desidera creare le credenziali, fare clic su Crea Nuovo. Per ulteriori informazioni sulla creazione di credenziali, consultare l'argomento Creazione di credenziali UNC (a pagina 463).

d. Fare clic su Salva.

Il percorso di archiviazione ed eliminazione è stato definito.

Creazione delle credenziali UNC

Le credenziali UNC si creano per consentire agli utenti di accedere alle risorse condivise dai server di CA SDM mediante il percorso UNC.

Importante. Il componente UNC non funziona quando il server CA SDM si trova nel dominio e la posizione condivisa è nel GRUPPO DI LAVORO. Non funziona nemmeno quando la password dell'amministratore per il server CA SDM e la posizione condivisa sono diversi.

Procedere come descritto di seguito:

1. Fare clic su Credenziali UNC nella pagina Impostazioni generali o selezionare Gestione protezione e ruoli, Credenziali UNC nella scheda Amministrazione.

   Viene visualizzata la pagina Elenco credenziali.

2. Fare clic su Crea Nuovo.

   Viene visualizzata la pagina Crea Nuove credenziali.

3. Completare i campi seguenti in modo appropriato:

   Simbolo

   Specifica l'ID univoco per identificare facilmente le credenziali durante una ricerca.

   Userid

   Specifica il nome utente per accedere al percorso UNC. L'utente può essere un utente locale o di dominio Windows con accesso al server di Service Desk.

   Password

   Specifica la password per accedere al percorso UNC.

   Attivo

   Specifica se le credenziali UNC sono attive. Non è possibile utilizzare le credenziali non attive.

4. Fare clic su Salva.

   Le credenziali UNC sono state create.

Selezione della regola di archiviazione ed eliminazione

È necessario selezionare la regola di archiviazione ed eliminazione appropriata. Considerare le possibilità seguenti:

- Creare una regola di archiviazione ed eliminazione (a pagina 530). Ad esempio, una regola di archiviazione ed eliminazione viene creata per i forum Gestione della conoscenza.
- Utilizzare una regola predefinita di archiviazione ed eliminazione (a pagina 533). Ad esempio, le regole predefinite si utilizzano per l'archiviazione e l'eliminazione dei dati KPI.

Creazione di una regola archiviazione ed eliminazione

Prima di poter eseguire l'archiviazione o l'eliminazione, creare una regola. La regola definisce gli elementi che si desiderano archiviare e il momento di esecuzione.

Esempio: Si crea una regola di archiviazione ed eliminazione per rimuovere i forum cancellati dal database.

Procedere come descritto di seguito:

1. Nella scheda Amministrazione, selezionare Archivia ed elimina, quindi Regole archiviazione ed eliminazione.

   Viene visualizzata la pagina Elenco Regole archiviazione ed eliminazione.

2. Fare clic su Crea Nuovo.

   Viene visualizzata la pagina Crea Nuova regola archiviazione ed eliminazione.

3. Compilare i campi della regola di archiviazione ed eliminazione (a pagina 531) in modo appropriato.
   - Selezionare il documento della conoscenza in Nome oggetto della configurazione.
   - Aggiungere KS_TYPE=20 in Query aggiuntiva.

4. Fare clic su Salva.

   La nuova regola viene visualizzata nella pagina Elenco Regole archiviazione ed eliminazione.

Esempio: Si crea una regola di configurazione facoltativa all'interno dei file arcpur_cfg.xml e itil_arcpur_cfg.xml per archiviare ed eliminare il nodo KPI_Ticket_Data.

Procedere come descritto di seguito:

1. Accedere al server seguente, a seconda della configurazione di CA SDM:
   - Convenzionale: server primario
   - Disponibilità avanzata: server in background

2. Individuare i file seguenti nella directory $NX_ROOT/site/cfg/:
   - arcpur_cfg.xml
   - itil_arcpur_cfg.xml
3. Modificare i file per definire end_time (last_mod_dt) nel nodo KPI_Ticket_Data. Specifica i criteri per selezionare i record per archiviazione e l'eliminazione.
4. Collegare i record della tabella KPI_Ticket_Data a quelli della tabella Ticket (come ad esempio cr, chg o iss). Ciò garantisce l'archiviazione e l'eliminazione di tutti i ticket correlati della tabella KPI_Ticket_Data.
5. Il nodo KPI_Ticket_Data non ha una relazione SREL (Relazione singola, Single Relation) con i nodi Ticket e utilizza due campi, obj_name e obj_id, per eseguire il collegamento a un ticket. Il valore di obj_name può essere cr, chg o iss, mentre il valore di obj_id è l'id del ticket. Definire un main_obj per ogni oggetto ticket.

   La seguente è una definizione campione main_object per l'oggetto ticket, cr:

   ```
   <!-- KPI Ticket Data -->

   <main_obj>

   <name>Dati Ticket KPI</name>

   <internal_name>Dati Ticket KPI</internal_name>

   <factory>ktd</factory>

   <default_query>obj_name='cr'</default_query>

   <date_field>end_time</date_field>

   <ref_by value="obj_id">cr.id</ref_by>

   </main_obj>
   ```

   Nota: la regola di configurazione può selezionare solo record per cr. Il tag ref_by può far corrispondere il valore di obj_id in Dati ticket KPI al valore di id in cr. Se viene trovata una corrispondenza, significa che un record Dati ticket KPI fa riferimento a un record cr, pertanto il record Dati ticket KPI non viene archiviato né eliminato.
6. Dopo aver aggiunto le regole di configurazione per tutti gli oggetti Ticket, a seconda della configurazione di CA SDM, compiere una delle azioni seguenti:
   - Riavviare i server di CA SDM per la configurazione convenzionale (a pagina 49).
   - Riavviare i server di CA SDM per la configurazione con disponibilità avanzata (a pagina 49).

   Queste regole di configurazione diventano nomi di oggetti di configurazione selezionabili nel modulo Dettagli regola archiviazione ed eliminazione.

Campi Regola archiviazione ed eliminazione

È possibile utilizzare i campi seguenti per definire o modificare le definizioni di regola.

Nome regola

Specifica un ID univoco per la regola.

Stato

Indica se la regola è attiva. La regola inattiva viene eseguita solo una volta, anche se è pianificata per un processo ricorrente.

Pianifica

Specifica il turno durante il quale la regola deve essere attiva.

Intervallo ricorrenza

Specifica la frequenza di esecuzione della regola.

Nome file archiviazione

Specifica il nome del file in cui si desidera memorizzare i record della cronologia. Immettere il nome del file specificato durante la definizione del percorso di archiviazione ed eliminazione. Per ulteriori informazioni, consultare la sezione Definizione del percorso di archiviazione ed eliminazione (a pagina 527).

Tipo operazione

Specifica uno dei seguenti tipi di operazione che deve essere eseguito dalla regola:

Archivia/Elimina

Archivia i record della cronologia in un file ed elimina i record archiviati dal database.

Elimina solamente

I record della cronologia vengono eliminati dal database ma non vengono scritti nel file di archiviazione.

Archivia solamente (Test)

I record della cronologia vengono scritti nel file di archiviazione senza essere eliminati dal database. Utilizzare questa opzione per verificare una regola di archiviazione ed eliminazione creata o modificata di recente.

Configurazione Nome oggetto

Specifica il nome dell'oggetto database che viene archiviato ed eliminato dalla regola. Il campo Nome oggetto viene compilato automaticamente in base alla selezione del campo Nome oggetto della configurazione.

Giorni di inattività

Consente di specificare il numero di giorni in cui un record non è attivo e non può essere selezionato per venire archiviato ed eliminato dal database.

Query aggiuntiva

Consente di archiviare ed eliminare specifici record non attivi tra quelli esistenti. Utilizzare questo campo per creare regole diverse per l'archiviazione e l'eliminazione di sottoinsiemi di record scaduti per lo stesso oggetto. Utilizzare la stessa sintassi di quella impiegata per le query memorizzate.

Ad esempio, la query seguente consente di archiviare ed eliminare solo i record di richieste non attive assegnate con priorità pari a 1:

```
priority = 1 AND (assignee IS NOT NULL OR group IS NOT NULL) and active = 0
```

Il seguente formato di query archivia e elimina i record in base a un intervallo di tempo:

```
close_date < EndAtTime(\'LAST_YEAR\')
```

Utilizzo di una regola predefinita di archiviazione ed eliminazione

È possibile utilizzare le regole predefinite in CA SDM per archiviare ed eliminare i dati della cronologia. Per impostazione predefinita, queste regole predefinite sono impostate su Non attivo. Impostare la regola su Attivo per utilizzarla.

Esempio: Utilizzare la regola predefinita per archiviare ed eliminare i dati KPI.

Procedere come descritto di seguito:

1. Nella scheda Amministrazione, selezionare Archivia ed elimina, quindi Regole archiviazione ed eliminazione.
2. Cercare una delle regole predefinite seguenti per i dati KPI:
   - Dati Ticket KPI
   - Dati KPI (Sistema)
   - Dati KPI (Query archiviata)
   - Dati KPI (SQL)
3. Selezionare la regola dal risultato della ricerca.
4. Fare clic su Modifica per modificare i campi della regola di archiviazione ed eliminazione (a pagina 531).

   Importante. Verificare di aver selezionato l'opzione Attivo dal campo Stato.
5. Fare clic su Salva.

   La regola predefinita è pronta per l'uso.

Verifica dei risultati di archiviazione ed eliminazione

Si controllano i risultati della regola pianificata di archiviazione ed eliminazione. Eseguire una o entrambe le azioni seguenti:

- Visualizzare la cronologia di archiviazione ed eliminazione (a pagina 534).
- Visualizzare il file di registro di archiviazione ed eliminazione.

Visualizzazione della cronologia di archiviazione ed eliminazione

È possibile visualizzare la cronologia per ogni regola di archiviazione ed eliminazione. Ad esempio, visualizzare gli oggetti eliminati per una regola.

Procedere come descritto di seguito:

1. Nella scheda Amministrazione, selezionare Archivia ed elimina e Cronologia archiviazione ed eliminazione.

   Viene visualizzata la pagina Elenco Cronologia archiviazione ed eliminazione.

2. Fare clic su Mostra filtro e specificare i criteri di filtro. Ad esempio, immettere la data di inizio meno recente per mostrare solo le voci dall'intervallo di tempo specificato.

   Nota: Per visualizzare il campo Altri argomenti di ricerca, fare clic sull'icona a forma di rubinetto. Si consiglia l'uso di questo campo solo da parte di utenti esperti, che conoscono i linguaggi SQL e Majic, per specificare altri argomenti di ricerca non previsti nell'area di ricerca. Per specificare un altro argomento di ricerca, immettere una clausola SQL WHERE in questo campo.

   Viene visualizzato l'elenco delle regole corrispondenti.

3. Fare clic sul nome della regola per cui si desidera esaminare la configurazione.

   Viene visualizzata la pagina Dettagli regola archiviazione ed eliminazione.

Visualizzare il file di registro di archiviazione ed eliminazione.

È possibile selezionare il file arcpur.log dalla directory $NX_ROOT/log/ per trovare gli errori riscontrati durante l'esecuzione della regola pianificata di archiviazione ed eliminazione.

Nota: La limitazione delle dimensioni per i file arcpur.log è definita in $NX_ROOT/NX.env come

```
# La dimensione massima per file di dati e file di registro di archiviazione ed
eliminazione.
@NX_ARCPUR_FILESIZE=2000000000
```

L'archiviazione e l'eliminazione creano arcpur.log.0, arcpur.log.1 attraverso arcpur.log.9 dopo che è stato raggiunto il limite per ciascun file di registro.

Ripristino dei dati archiviati

È possibile ripristinare i dati archiviati quando sono nuovamente necessari nel database.

Procedere come descritto di seguito:

1. Avviare i daemon in modalità dbadmin. La modalità dbadmin consente l'accesso limitato, in modo da poter eseguire senza problemi pdm_load per ripristinare i dati archiviati. Eseguire il comando pdm_d_mgr -s DBADMIN sui server seguenti, a seconda della configurazione di CA SDM:
   - Convenzionale: server primario
   - Disponibilità avanzata: server in background
2. Accedere alla directory principale o alla posizione UNC di memorizzazione dei dati archiviati.
3. Individuare il file dei dati archiviati (file .dat).
4. Copiare il file nei server seguenti, a seconda della configurazione di CA SDM:
   - Convenzionale: server primario
   - Disponibilità avanzata: server in background
5. Eseguire pdm_load sul file di dati. Ad esempio:
   `pdm_load -a -f 2004611T1726_Call_Request.dat`
6. In caso di problemi con il comando pdm_load, completare i passaggi seguenti:
   a. Selezionare la riga di comando $NX_ROOT/log/arcpur.log per errori.
   b. Riavviare i server di CA SDM (a pagina 49).
7. Per evitare che il record venga archiviato ed eliminato al ciclo successivo, procedere come segue:
   a. Aggiornare il record per renderlo di nuovo attivo.
   b. Disattivare la regola associata di archiviazione ed eliminazione.

Miglioramento delle prestazioni con la cache del browser

L'interfaccia Web di CA SDM utilizza molti file JavaScript, CSS e di immagine, le cui dimensioni possono essere considerevoli, con ripercussioni sulle prestazioni dell'interfaccia stessa.

Per migliorare le prestazioni dell'interfaccia Web, impostare il server HTTP in modo tale da caricare tali file nella cache del browser dell'utente una sola volta al giorno.

Le prestazioni dell'interfaccia Web migliorano nettamente.

Nota: per impostazione predefinita, il caricamento nella cache avviene automaticamente nei sistemi Apache e IIS, ma è possibile configurarlo manualmente.

Configurazione di Microsoft Internet Information Server

È possibile configurare Microsoft Internet Information Server (IIS) per notificare al browser che i file caricati dalla directory CA SDM scadono un giorno dopo il caricamento. Ciò significa che il browser richiede i file al server solo una volta al giorno, indipendente dal numero di volte che vengono utilizzati.

Per configurare Microsoft Internet Information Server

1. Avviare Gestione servizio Internet (in Windows 2000 e XP, selezionare Programmi, Strumenti di amministrazione, Gestione servizio Internet).
2. Accedere alla cartella di CA SDM, solitamente denominata CAisd:
    a. Fare clic sul segno più (+) accanto al server su cui è eseguita l'interfaccia Web di CA SDM.
    b. Fare clic sul segno più (+) accanto a Sito Web predefinito.
    c. Scorrere fino a CAisd.
3. Fare clic con il pulsante destro del mouse sulla cartella CAisd e selezionare Proprietà.

    Viene visualizzata la pagina Proprietà.
4. Fare clic sulla scheda Intestazioni HTTP.
5. Fare clic sulla casella di controllo Abilita scadenza contenuto.
6. Selezionare il pulsante di opzione Dopo, immettere 1 nel campo di testo e scegliere il giorno dall'elenco a discesa.
7. Fare clic su OK.

    Le proprietà vengono salvate e le modifiche hanno effetto immediatamente.

Configurazione di Apache

È possibile configurare Apache per notificare al browser che i file caricati dalla directory CA SDM scadono un giorno dopo il caricamento. Impostando questa configurazione il browser richiede i file al server solo una volta al giorno, indipendentemente dal numero di volte che vengono utilizzati.

Per configurare il sistema Apache, è necessario aggiornare un file di configurazione in formato testo. L'installazione predefinita richiede l'aggiunta della seguente istruzione al file di configurazione attivo nella directory di configurazione di Apache (solitamente httpd.conf):

```
Include directory_installazione/bopcfg/www/CAisd_apache.conf
```

directory_installazione deve essere sostituito con un percorso completo. In Windows, il percorso in genere è c:\Programmi\CA\CA SDM. In UNIX, sostituire *directory-installazione* con il valore $NX_ROOT.

Il file CAisd_apache.conf a cui si riferisce l'istruzione Include contiene il testo indicato di seguito. *directory-installazione* viene sostituita di nuovo con il percorso completo utilizzato per l'istruzione Include.

```
<IfModule mod_alias.c>
        Alias /CAisd directory_installazione/bopcfg/www/wwwroot/
        <IfModule mod_expires.c>
                <Directory directory_installazione/bopcfg/www/wwwroot>
                ExpiresActive   On
                ExpiresDefault  "access plus 1 day"
                </Directory>
        </IfModule>
</IfModule>
```

Per configurare manualmente il sistema Apache per il caricamento dei file di CA SDM nella cache del browser, includere istruzioni simili a quelle presenti in CAisd_apache.conf nel file di configurazione Apache. È possibile aggiungere le istruzioni direttamente nel file oppure aggiungere un'istruzione Include che fa riferimento a un file separato, ad esempio il file dell'installazione predefinita.

Le modifiche ai file di configurazione Apache vengono applicate solo dopo il riavvio del sistema Apache.

Cancellazione della cache

Se si modificano JavaScript, immagini, fogli di stile, HTML o file della Guida caricati dal server HTTP, è necessario richiedere agli utenti di cancellare la cache del browser.

Nota: per applicare le modifiche apportate ai file HTMPL, è necessario riavviare il motore Web o usare l'utilità pdm_webcache. In un ambiente di sviluppo, è possibile evitare questa operazione specificando la proprietà del file di configurazione SuppressHtmplCache.

Per cancellare la cache del browser in Internet Explorer

1. Selezionare Strumenti->Opzioni Internet.

   Viene visualizzata la finestra di dialogo Opzioni Internet.

2. Fare clic su Elimina file.

   Viene visualizzata una finestra di conferma.

3. Fare clic su OK.

   La cache del browser verrà cancellata.

Per cancellare la cache del browser in Firefox

1. Selezionare Strumenti, Cancella cronologia recente.
2. Fare clic sul pulsante Cancella adesso.

   La cache del browser verrà cancellata.

Modifica del file di configurazione

Durante l'installazione dell'interfaccia Web di CA SDM, viene installato un file di configurazione del motore Web di esempio (*web.cfg*). È possibile modificare questo file in base alle proprie necessità. Il file *web.cfg* contiene commenti utili che si possono consultare durante la lettura del file. È possibile il file *web.cfg* dalla directory appropriata:

- (Windows) %NX_ROOT%\bopcfg\www\
- (UNIX) $NX_ROOT/bopcfg/www/

Nota: in Gestione Opzioni sono disponibili alcune variabili di configurazione aggiuntive, come ad esempio charset. È possibile accedervi mediante la scheda Amministrazione dell'interfaccia Web. Per ulteriori informazioni, consultare la *Guida in linea*.

AllowInactiveSrelEntry

Specifica se è possibile salvare un record quando fa riferimento a record non attivi in una tabella di riferimenti.

- Se questa proprietà viene omessa oppure impostata su zero, le voci non attive della tabella dei riferimenti (ad esempio, lo stato di una richiesta oppure una categoria di modifica) non vengono incluse negli elenchi di selezione e non possono essere specificate per le ricerche o nei campi di ricerca gerarchica.
- Se questa proprietà viene impostata su 1, il flag "non attivo" viene ignorato nelle voci della tabella dei riferimenti.

Indipendentemente dall'impostazione del flag, i record che contengono già un riferimento a una voce non attiva della tabella dei riferimenti possono essere salvati senza modificare il riferimento. Il flag influisce solo sui nuovi valori di campo.

AnnouncementLength

Specifica il numero di annunci da visualizzare nella finestra di apertura nelle interfacce dei clienti e degli analisti. CA SDM visualizza l'annuncio più recente, quindi il numero di annunci specificato da questo parametro. L'interfaccia degli analisti consente di visualizzare altri annunci tramite l'opzione Annunci del menu Cerca.

Impostazione predefinita: 10, ovvero vengono visualizzati i dieci annunci più recenti.

AnonymousPrio

Specifica priorità valide per ticket creati da utenti guest. Questi utenti possono specificare solo una delle priorità nell'elenco AnonymousPrio per i propri ticket. Le voci nell'elenco delle priorità sono separate da spazi. Ciascuna voce deve essere un numero compreso tra 1 e 5 oppure la parola "nessuna" (senza virgolette). La priorità predefinita per i ticket creata dagli utenti di tipo guest deve essere specificata per prima e può essere ripetuta nell'elenco.

I valori validi per la proprietà AnonymousPrio corrispondono ai nomi simbolici delle proprietà distribuite. È possibile utilizzare il client Java per personalizzare i nomi simbolici. Tuttavia, la personalizzazione non ha effetto sulla specifica della proprietà AnonymousPrio, che deve continuare a fare riferimento alle priorità in base ai propri nomi predefiniti, dove 1 corrisponde alla priorità più alta.

Impostazione predefinita: nessuna, ovvero nessuna richiesta creata da un utente guest ha priorità.

Riempimento automatico

Specifica che l'interfaccia Web deve completare automaticamente i campi di ricerca quando un utente inserisce dati in un campo e preme il tasto di tabulazione per passare a un altro campo. Quando un utente preme il tasto di tabulazione e se l'opzione Riempimento automatico è selezionata, il browser richiede al server di confermare che l'aggiornamento sia corretto. Come risultato, il nome completo viene automaticamente inserito nel campo (se l'utente aveva specificato un nome parziale) oppure viene visualizzata una finestra di ricerca (se la selezione dell'utente non era valida o era ambigua).

Questa proprietà è opzionale. La proprietà Autofill è attivata per impostazione predefinita. Se viene omessa oppure impostata su Yes, quando si preme il tasto di tabulazione per uscire da un campo di ricerca, viene automaticamente eseguita la ricerca nel database. Se questa proprietà è impostata su No, nessun campo viene completato automaticamente e i campi di ricerca non vengono verificati fin quando il record non viene salvato.

CAisd

Specifica il percorso (inclusa una barra iniziale) dell'alias o della directory virtuale nel server HTTP che contiene i file richiesti dal server Web di CA SDM. Solitamente, il valore di questa proprietà è /CAisd sia in UNIX sia in Windows. Per i server Apache, il valore deve essere definito nell'istruzione Alias di un file di configurazione. Per IIS, il valore deve corrispondere al campo Alias della finestra Proprietà directory.

CGI

Specifica il nome del programma eseguibile CGI fornito con l'interfaccia Web (senza suffisso .exe).

Impostazione predefinita: pdmweb

Nota: se viene rinominato questo programma, è necessario aggiornare questa proprietà.

CgiReport

Specifica il nome del programma eseguibile CGI per i report Web fornito con l'interfaccia Web (senza suffisso .exe).

Impostazione predefinita: pdm_cgireport

Nota: se viene rinominato questo programma, è necessario aggiornare questa proprietà.

ContactAutoDesc

Specifica se il nome del contatto deve essere inserito nella descrizione delle nuove questioni e richieste create nelle interfacce dei clienti e dei dipendenti. Se questa proprietà viene omessa oppure impostata su 0, non vengono aggiunte automaticamente informazioni alla descrizione delle nuove questioni e richieste. Se questa proprietà viene impostata su 1, il nome del contatto viene automaticamente inserito nella descrizione delle nuove questioni e richieste create nelle interfacce dei clienti e dei dipendenti. Questa proprietà non ha alcun effetto sull'interfaccia degli analisti.

ContactAutoDescWithIP

Specifica se l'indirizzo IP del contatto deve essere inserito nella descrizione delle nuove questioni e richieste create nelle interfacce dei clienti e dei dipendenti. Se questa proprietà viene omessa oppure impostata su 0, l'indirizzo IP non viene aggiunto alla descrizione delle nuove questioni e richieste. Se questa proprietà e la proprietà ContactAutoDesc sono entrambe impostate su 1, il nome del contatto e l'indirizzo IP vengono automaticamente inseriti nella descrizione delle nuove questioni e richieste create nelle interfacce dei clienti e dei dipendenti. Questa proprietà non ha alcun effetto sull'interfaccia degli analisti. Viene ignorata a meno che il valore della proprietà ContactAutoDesc non sia 1.

CstPrio

Priorità valide per le questioni create con l'interfaccia Web dei clienti. Per le loro questioni, gli utenti che utilizzano l'interfaccia dei clienti possono specificare solo una delle priorità riportate nell'elenco CstPrio e non possono aggiornare la priorità di una questione se un analista ha cambiato il valore con uno non disponibile nell'elenco.

Le voci nell'elenco delle priorità sono separate da spazi. Ciascuna voce deve essere un numero compreso tra 1 e 5 oppure la parola "nessuna" (senza virgolette). La priorità predefinita delle questioni create con l'interfaccia dei clienti deve essere specificata per prima e può essere ripetuta nell'elenco.

Impostazione predefinita: niente, 3, 4, 5

I valori validi per la proprietà CstPrio corrispondono ai nomi simbolici delle proprietà distribuite. È possibile utilizzare il client Java per personalizzare i nomi simbolici. Tuttavia, la personalizzazione non ha effetto sulla specifica della proprietà CstPrio, che deve continuare a fare riferimento alle priorità in base ai propri nomi predefiniti, dove 1 corrisponde alla priorità più alta.

DateFormat

Definisce l'ordine degli elementi nelle date.

Impostazione predefinita: GG/MM/AAAA hh:mm a(am,pm)

Simbolo	Descrizione
M	1 o 2 cifre per indicare il mese
MM	2 cifre per indicare il mese
D	1 o 2 cifre per indicare il giorno
DD	2 cifre per indicare il giorno
YY	2 cifre per indicare l'anno
YYYY	4 cifre per indicare l'anno
H	1 o 2 cifre per indicare l'ora (orologio basato su 24 ore)
HH	2 cifre per indicare l'ora (orologio basato su 24 ore)
H	1 o 2 cifre per indicare l'ora (orologio basato su 12 ore)
hh	2 cifre per indicare l'ora (orologio basato su 12 ore)
M	1 o 2 cifre per indicare i minuti
mm	2 cifre per indicare i minuti
A	1 o 2 cifre per indicare i secondi
ss	2 cifre per indicare i secondi
a(am, pm)	"am" e "pm" in formato stringa

DateFormatNoTime

Specifica la stessa definizione di DateFormat, ma non la parte relativa all'ora.

DebugSource

Abilita il menu di scelta rapida standard del browser nei moduli di CA SDM. Se questa proprietà non viene impostata, facendo clic con il pulsante destro del mouse su un modulo viene visualizzato il menu di CA SDM. Prestare attenzione quando si imposta questa proprietà. Alcune opzioni dei menu di scelta rapida standard del browser potrebbero causare errori di esecuzione. Questo è il motivo per cui solitamente questa proprietà è disattivata. In Internet Explorer, è possibile visualizzare il menu di scelta rapida standard del browser, anche quando la proprietà DebugSource non è impostata, premendo il tasto Ctrl quando si fa clic con il pulsante destro del mouse.

DebugTrace

Fa in modo che il motore Web scriva le informazioni di traccia nel file stdlog.

Importante Questa proprietà *non* dovrebbe essere impostata per uso normale. Dovrebbe essere utilizzata solo quando richiesto da CA Support.

EmpPrio

Priorità valide per le richieste create con l'interfaccia Web dei dipendenti. Per le loro richieste, gli utenti che utilizzano l'interfaccia dei dipendenti possono specificare solo una delle priorità riportate nell'elenco EmpPrio e non possono aggiornare la priorità di una richiesta se un analista ha cambiato il valore con uno non disponibile nell'elenco.

Le voci nell'elenco delle priorità sono separate da spazi. Ciascuna voce deve essere un numero compreso tra 1 e 5 oppure la parola "nessuna" (senza virgolette). La priorità predefinita delle richieste create con l'interfaccia dei dipendenti deve essere specificata per prima e può essere ripetuta nell'elenco.

Predefinito: niente, 3, 4, 5

I valori validi per la proprietà EmpPrio corrispondono ai nomi simbolici delle proprietà distribuite. È possibile utilizzare il client Java per personalizzare i nomi simbolici. Tuttavia, la personalizzazione non ha effetto sulla specifica della proprietà EmpPrio, che deve continuare a fare riferimento alle priorità in base ai propri nomi predefiniti, dove 1 corrisponde alla priorità più alta.

ExclLockSeconds

Specifica il numero massimo di secondi in cui l'utente è il proprietario esclusivo di un record dopo aver fatto clic su Modifica (il record viene bloccato). Trascorso il periodo, il motore Web rilascia il blocco consentendo agli altri utenti di aggiornare il record. Il motore Web tenta di mantenere il blocco se l'utente richiede il salvataggio dopo che è scaduto il tempo specificato nella proprietà ExclLockSeconds. Il tentativo riesce solo se nessun altro utente ha nel frattempo aggiornato il record. Se il tentativo di mantenere il blocco non riesce, l'utente deve immettere nuovamente gli aggiornamenti.

Impostazione predefinita: 120 (due minuti)

Questo argomento è opzionale. Se omesso, viene utilizzato il valore predefinito.

Nota: il valore della proprietà ExclLockSeconds deve essere inferiore a quello della proprietà Timeout. La proprietà ExclLockSeconds è espressa in secondi, mentre la proprietà Timeout è espressa in minuti.

FormCacheMax

Specifica il numero massimo di moduli che deve essere mantenuto nella memoria del motore Web per ciascun utente. Il motore Web mantiene sempre gli ultimi moduli (il numero è specificato nella proprietà FormCacheMax) utilizzati da ciascun utente. Oltre questo numero, i moduli possono essere considerati scaduti. Una volta scaduti, non è più possibile accedere ai moduli con i pulsanti Indietro e Avanti nella pagina principale. Inoltre, questi moduli non possono essere più inviati a un modulo popup.

Impostazione predefinita: 10

I moduli scaduti, poiché vengono eliminati dalla cache, consentono di risparmiare memoria del motore Web. Tuttavia, a volte possono richiedere l'aggiornamento manuale da parte degli utenti. È possibile impostare la proprietà FormCacheMax sul valore –1 per disattivare la funzionalità di scadenza dei moduli.

FormTimeout

Specifica il numero minimo di secondi che un modulo viene mantenuto nel motore Web prima di essere considerato idoneo per la rimozione della cache. Gli utenti dispongono sempre almeno del tempo specificato in questo parametro per lavorare su un modulo prima di inviarlo. Inoltre, il motore Web mantiene sempre gli ultimi moduli utilizzati (in base al valore della proprietà FormCacheMax) per ogni utente.

È possibile utilizzare la proprietà StayCacheList per impedire il timeout di moduli specifici.

Impostazione predefinita: 180 (3 minuti)

FormTitle

Specifica una stringa da includere nella barra del titolo del browser Web che visualizza i moduli Web di CA SDM. Il valore della proprietà FormTitle si aggiunge al titolo del modulo specifico correntemente visualizzato.

Impostazione predefinita: CA SDM

Ad esempio, se si mantiene il valore predefinito e si utilizza Microsoft Internet Explorer come browser per la visualizzazione del modulo Dettagli annuncio, la barra del titolo risulta:

Dettagli annuncio — CA SDM — Microsoft Internet Explorer

Questa proprietà è opzionale. Se omessa, l'interfaccia Web degli analisti non utilizza un valore costante nella barra del titolo. Le interfacce Web dei clienti e PDA tornano al valore predefinito.

HitTrackFile

Specifica il percorso completo del file che riceve una registrazione di tutte le pagine Web utilizzate. In questo file viene scritta una riga ogni volta che un utente richiede una pagina. Le dimensioni del file possono aumentare all'infinito, pertanto utilizzare questa proprietà con estrema attenzione.

Nota: i record che contengono data e ora, l'ID utente, l'ID record del database e il nome del modulo HTMPL vengono aggiunti alla fine del file. Il formato dei record può variare. È necessario intervenire periodicamente su questo file, in modo da controllarne le dimensioni.

Questa proprietà è opzionale. Se omessa, il file di traccia non viene scritto.

HtmplCacheSize

Specifica la dimensione della cache HTMPL. Quando questa dimensione è superata, il modulo meno recente viene rimosso dalla cache.

Impostazione predefinita: 1000.

ListAllMaximum

Specifica il numero massimo di record presenti in un elenco prima della visualizzazione di un messaggio di avvertenza che informa gli utenti che la richiesta non è consentita poiché ha un impatto negativo sulle prestazioni, a seguito di una richiesta di visualizzazione dell'intero elenco.

Impostazione predefinita: 2500

ListAllWarn

Specifica il numero massimo di record presenti in un elenco prima della visualizzazione di un messaggio di avvertenza che informa gli utenti che la richiesta potrebbe avere un impatto negativo sulle prestazioni, a seguito di una richiesta di visualizzazione dell'intero elenco. Viene richiesto di confermare se procedere.

Impostazione predefinita: 1000

ListBottomMaximum

Specifica il numero massimo di record presenti in un elenco prima della visualizzazione di un messaggio di avvertenza che informa gli utenti che la richiesta non è consentita poiché ha un impatto negativo sulle prestazioni, a seguito di una richiesta di scorrere fino in fondo.

Predefinito: 2500

ListBottomWarn

Specifica il numero massimo di record presenti in un elenco prima della visualizzazione di un messaggio di avvertenza che informa gli utenti che la richiesta potrebbe avere un impatto negativo sulle prestazioni, a seguito di una richiesta di scorrere fino in fondo. Viene richiesto di confermare se procedere.

Predefinito: 1000

ListPageLength

Specifica il numero massimo di record trovati da mostrare in una pagina di elenco dopo una ricerca.

Impostazione predefinita: 10

LogoutURL

Specifica l'URL completo di una pagina Web da visualizzare dopo la disconnessione da CA SDM. Questa proprietà è opzionale. Se omessa, a seguito della disconnessione viene visualizzato nuovamente il modulo di accesso.

Lr_Refresh

Specifica l'intervallo di aggiornamento del lettore registro, in secondi. Se il valore di questa proprietà è diverso da 0, la funzione Lettore registro notifiche si aggiorna automaticamente in base all'intervallo specificato. Il valore minimo è 30 secondi.

Questa proprietà è opzionale. Se omessa, il lettore registro si aggiorna ogni 5 minuti (valore predefinito pari a 300 secondi). Se il valore di questa proprietà è 0, il lettore registra non si aggiorna mai automaticamente.

MacroPath

Specifica un elenco di percorsi di directory in cui il motore Web ricerca i file richiesti dal tag PDM_MACRO. È possibile specificare più directory, separandole con spazi. È possibile includere le variabili di ambiente nei nomi delle directory, utilizzando il simbolo del dollaro come prefisso (ad esempio, $NX_ROOT). Per Windows e UNIX, separare ogni percorso con la barra (/) e non con la barra rovesciata (\). Questa proprietà è obbligatoria. Solitamente, l'impostazione è:

```
$NX_ROOT/site/mods/macro $NX_ROOT/bopcfg/www/macro
```

MatchesFound

Specifica il testo del messaggio da visualizzare sotto un campo quando la chiave utente per un campo di ricerca è ambigua ed è necessario visualizzare nuovamente il modulo di modifica con un elenco di selezione. Questa proprietà è opzionale. Se omessa, il valore predefinito è Più corrispondenze.

MaxRecordsAutoSuggest

Specifica il numero di record visualizzati dal suggerimento automatico al di sotto di un elemento di ricerca.

Valore predefinito: 25

MaxSelectList

Specifica il numero massimo di corrispondenze da visualizzare nell'elenco di selezione quando una chiave utente per un campo di ricerca è ambigua ed è necessario visualizzare nuovamente il modulo di modifica. Se vengono rilevate molte altre corrispondenze, viene visualizzato il messaggio Troppe corrispondenze.

MinCharsAutoSuggest

Specifica il numero minimo di caratteri da inserire nei campi di ricerca prima della visualizzazione dei suggerimenti automatici.

Valore predefinito: 3

MouseoverPreviewDelayTime

Specifica l'intervallo di tempo (in millisecondi) tra il posizionamento del mouse su un collegamento e la visualizzazione dell'anteprima corrispondente.

Se il mouse viene spostato dal collegamento prima dell'intervallo di tempo specificato, l'anteprima non verrà visualizzata.

Valore predefinito: 1000

NoMatchesFound

Specifica il testo del messaggio da visualizzare sotto un campo quando la chiave utente per un campo di ricerca non è valida ed è necessario visualizzare nuovamente il modulo di modifica. Questa proprietà è opzionale. Se omessa, il valore predefinito è Nessuna corrispondenza trovata.

PreLogin Timeout

Specifica il numero massimo di minuti durante i quali il motore Web mantiene attiva una sessione prima dell'accesso. Il motore Web avvia automaticamente una sessione quando un utente richiede un modulo di accesso, prima che l'utente completi il processo di accesso. Se l'utente non completa l'accesso entro il tempo specificato, il motore Web annulla la sessione. Se l'utente ripete la richiesta di accesso, il motore Web avvia una sessione. Questa operazione è trasparente all'utente.

Questa proprietà non ha alcun impatto sull'utente finale. È una proprietà che ottimizza le prestazioni, bilanciando l'uso della memoria del motore Web rispetto al sovraccarico che deriva dalle operazioni di annullamento e nuova apertura delle sessioni. Questa proprietà è opzionale. Se omessa, il valore predefinito è 1 minuto.

RedirectingURL

Specifica l'URL che il Web Director deve utilizzare per inviare le richieste a questo motore Web. Questa proprietà specifica l'URL completo del motore Web (http incluso). Questa proprietà è obbligatoria se si utilizza il Web Director. In caso contrario, viene ignorata.

SchedExpMaximum

SchedExpMaximum

Specifica il numero massimo di pianificazioni che è possibile esportare contemporaneamente.

Impostazione predefinita: 1000

Importante L'impostazione predefinita corrisponde al numero massimo di esportazioni che CA SDM è in grado di gestire contemporaneamente. Incrementare il valore predefinito può causare instabilità di sistema. Se si tenta di esportare un numero maggiore di eventi rispetto al valore specificato in SchedExpMaximum, viene visualizzato un messaggio che informa dell'impossibilità di eseguire l'esportazione.

SelListCacheExclude

SelListCacheExclude

Specifica i nomi degli oggetti (factory) da escludere dal processo di inserimento nella cache per gli elenchi <PDM_SELECT>. Per migliorare le prestazioni, normalmente il motore Web carica nella propria memoria cache il contenuto di piccole tabelle utilizzate negli elenchi di selezione <PDM_SELECT> e negli elenchi di ricerca gerarchica. È possibile impedire che una particolare tabella venga caricata nella cache se alla partizione dati in uso sono applicati vincoli per specificare gruppi di utenti a cui devono essere visualizzate viste diverse della tabella. Inoltre, la specifica delle tabelle nel valore di questa proprietà elimina la necessità per il motore Web di richiedere il numero dei record all'avvio, migliorando leggermente le prestazioni all'avvio. Questa proprietà è opzionale. Se specificata, deve contenere uno o più nomi di oggetti separati da spazi.

SelListCacheMax

SelListCacheMax

Definisce il numero massimo di record di tabella che possono essere caricati nella cache del motore Web. Il motore Web mantiene nella propria memoria l'intero contenuto delle tabelle o parte di esse (in base alla dimensione della cache), migliorando le prestazioni relative alla creazione degli elenchi <PDM_SELECT> che si basano su queste tabelle. Un valore molto alto di questa proprietà, significa un miglioramento delle prestazioni ma un aumento dell'utilizzo della memoria.

Impostazione predefinita: 10

La proprietà SelListCacheMax viene ignorata per le tabelle utilizzate negli elenchi di ricerca gerarchica, ad esempio le categorie per le richieste, le questioni e gli ordini di cambiamento. Il motore Web mantiene sempre nella propria memoria l'intero contenuto delle tabelle utilizzate negli elenchi di ricerca gerarchica. Se queste tabelle contengono un numero elevato di valori, è possibile specificare la proprietà SelListCachePreload.

SelListCachePreload

Specifica una o più tabelle che devono essere caricate all'avvio nella cache di selezione del motore Web. Le tabelle che non vengono specificate in questa proprietà vengono caricate solo la prima volta che vengono utilizzate. Se la proprietà SelListCacheMax è impostata su un valore alto oppure se l'elenco di ricerca gerarchica (ad esempio, una categoria) contiene un numero elevato di record, è consigliabile specificare la tabella nella proprietà SelListCachePreload. In questo modo, si evitano tempi lunghi di risposta la prima volta che un utente accede a un modulo che utilizza la tabella.

Il valore della proprietà SelListCachePreload è un elenco di nomi di oggetto separati da spazi. Ogni nome di oggetto può essere seguito da un elenco opzionale di nomi di attributi racchiusi tra parentesi. Gli attributi specificati nell'elenco vengono caricati nel motore Web. Se non specificati attributi, vengono caricati solo il nome comune e il valore di attributo relativo dell'oggetto. Queste informazioni sono sufficienti per gli elenchi di selezione, ma non lo sono per le ricerche gerarchiche. Se si modificano i moduli di ricerca gerarchica, (hiersel_xx.htmpl, dove xx è un nome di oggetto), assicurarsi che nella proprietà SelListCachePreload siano specificati tutti gli attributi utilizzati nel modulo. Se si omette un attributo, la cache viene ricaricata al momento dell'utilizzo del modulo.

La proprietà SelListCachePreload è opzionale. Se viene omessa, non viene caricato nulla nella cache di selezione fino a quando un utente non richiede un modulo utilizzando un elenco di selezione o una ricerca gerarchica.

```
chgcat(description owning_contract) chgstat crs isscat(description
owning_contract) issstat pcat(description cr_flag in_flag pr_flag
owning_contract) pri tskstat urg pcat_cr(description cr_flag in_flag pr_flag
owning_contract) pcat_pr(description cr_flag in_flag pr_flag owning_contract)
pcat_in(description cr_flag in_flag pr_flag owning_contract)
```

StayCacheList

Specifica i nomi di moduli che non devono essere mai rimossi dalla cache dei moduli, indipendentemente dal tempo in cui rimangono visualizzati. Questa proprietà assicura che i frame fissi di una vista basata su frame rimangano sempre visualizzati in una sessione. È una proprietà da utilizzare con molta attenzione perché si potrebbe per errore specificare moduli che rimarrebbero sempre caricati nella cache. Il valore predefinito è:

```
scoreboard.htmpl top_splash.htmpl buttons.htmp hiersel_admin_tree.htmpl
```

SuppressHtmplCache

Specifica che il motore Web deve rileggere tutti i file che definiscono il contenuto di una pagina ogni volta che la pagina viene richiesta. L'analisi di un file HTMPL richiede un tempo di elaborazione estremamente lungo e solitamente richiede la lettura di diversi file fisici, dal momento che la maggior parte dei tag utilizza PDM_INCLUDE. Il motore Web normalmente salva i file analizzati nella propria memoria in modo che le richieste future della stessa pagina possano essere soddisfatte immediatamente. Questo metodo migliora in modo significativo le prestazioni, ma può costituire un inconveniente per gli utenti che si occupano dello sviluppo di nuove pagine e dell'aggiornamento delle pagine esistenti. Per applicare le modifiche, è necessario riavviare il motore Web.

Questa proprietà è opzionale e non richiede alcun valore. Se viene specificata, il motore Web non inserisce nella cache i file analizzati e le modifiche ai file HTMPL vengono applicate immediatamente. A causa dell'impatto sulle prestazioni, questa proprietà non deve essere specificata in un ambiente di produzione.

SuppressLoginAndLogoutMsg

Specifica che il motore Web non deve registrare un messaggio nel file registro di CA SDM ogni volta che un utente accede o si disconnette dall'interfaccia Web.

Questa proprietà è opzionale. Se non viene specificata, il motore Web registra un messaggio ogni volta che un utente esegue l'accesso o la disconnessione.

SuppressMacroCache

Specifica che il motore Web deve eliminare tutte le macro salvate ogni volta che una nuova pagina viene richiesta. Il motore Web normalmente salva le macro analizzate nella propria memoria in modo che le richieste future delle stesse macro possano essere soddisfatte immediatamente. Questo metodo migliora in modo significativo le prestazioni, ma può costituire un inconveniente per gli utenti che si occupano dello sviluppo di nuove macro e dell'aggiornamento delle macro esistenti. Per applicare le modifiche, è necessario riavviare il motore Web.

Questa proprietà è opzionale. Se viene specificata, il motore Web non inserisce nella cache le macro analizzate e le modifiche alle macro vengono applicate immediatamente. A causa dell'impatto sulle prestazioni, questa proprietà non deve essere specificata in un ambiente di produzione.

Timeout

Specifica il numero di minuti durante i quali una sessione utente può rimanere inattiva prima che venga automaticamente terminata, liberando tutte le risorse del server.

Nota: il valore della proprietà Timeout deve essere superiore a quello della proprietà ExclLockSeconds. La proprietà ExclLockSeconds è espressa in secondi, mentre la proprietà Timeout è espressa in minuti.

TooManyMatches

Specifica il testo del messaggio da visualizzare sotto un campo quando la chiave utente per un campo di ricerca è ambigua e il numero di corrispondenze della chiave supera il valore di MaxSelectList. Questa proprietà è opzionale. Se omessa, il valore predefinito è Troppe corrispondenze.

UpdatedAnnouncementsPopup

La frequenza con cui il browser controlla la disponibilità di nuovi annunci. Quando viene rilevato un nuovo annuncio, il browser lo visualizza automaticamente in una finestra. Il valore dell'intervallo è espresso in minuti. Per ridurre l'impatto sulle prestazioni del browser, si consiglia di impostare questa variabile su un valore maggiore di 5 (minuti).

UseDirector

Specifica quando il Web Director controlla il motore Web. La tabella seguente riporta i possibili valori:

Valore	Descrizione
No	Il motore Web è indipendente dal Web Director. Si tratta del valore predefinito.
Sì	Il Web Director deve avviare tutte le sessioni, incluso il modulo di accesso. Se un utente tenta l'accesso diretto al motore Web, il motore Web richiede al Web Director un riferimento di tale utente.
AfterLogin	Il motore Web segnala una sessione al Web Director dopo l'autenticazione di un utente. Un motore Web configurato con il parametro UseDirector AfterLogin è responsabile solo dell'autenticazione. Pertanto, è un motore adatto per l'uso del protocollo SSL ai fini della massima protezione.
BeforeLogin	Il motore Web segnala una sessione al Web Director prima dell'autenticazione di un utente. Un motore Web configurato con il parametro UseDirectory BeforeLogin non visualizza mai la pagina di accesso e non accetta mai una password di accesso.

Questa proprietà è opzionale. Se omessa, il motore Web non utilizza il Web Director.

UseNestedTabs

Specifica se visualizzare il controllo delle schede nidificate nei moduli dettagli.

Impostazione predefinita: Abilitato

WebDirectorSlumpName

Specifica il nome del Web Director che si occupa della gestione del motore Web. Questa proprietà è richiesta solo se si utilizza più di un Web Director oppure se il Web Director è stato configurato con un nome slump diverso da quello predefinito (web:director).

Questa proprietà è opzionale se si utilizza il Web Director. In caso contrario, viene ignorata.

WillingnessValue

Specifica la disponibilità del motore Web ad accettare sessioni, su una scala da 0 a 10. Questa proprietà è disponibile solo se si utilizza il Web Director. Questo valore ha importanza solo se messo a confronto con la disponibilità degli altri motori Web associati allo stesso Web Director. Il Web Director trasferisce le sessioni ai motori Web in base ai propri valori di disponibilità. Un motore Web con valore di disponibilità doppio rispetto a quello di un altro motore Web, gestisce in media il doppio del numero di sessioni.

Se il valore della proprietà WillingnessValue è 0, significa che il motore Web non accetta le sessioni. Questo valore può essere utile se UseDirector è AfterLogin.

Questa proprietà è opzionale se si utilizza il Web Director. In caso contrario, viene ignorata. Se omessa, il valore predefinitè è 5.

WorkFrameTimeout

Specifica il numero massimo di secondi durante i quali il motore Web attende la risposta per una richiesta del server interna prima di considerare la richiesta come non riuscita. La finestra temporale viene utilizzata per le funzioni dell'interfaccia Web di CA SDM che richiedono al server dati diversi dalle normali pagine Web. Tra le funzioni sono incluse il riempimento automatico, il caricamento delle proprietà delle categorie e l'aggiornamento dei segnapunti. Le richieste inviate a CA SDM difficilmente non vengono soddisfatte. Tuttavia, le stesse richieste inoltrate ad altri server (ad esempio, prodotti integrati quali Gestione della conoscenza) potrebbero non riuscire se il server interessato non è in esecuzione oppure se ci sono problemi di rete che impediscono l'accesso ad esso. La proprietà WorkFrameTimeout specifica un intervallo di tempo oltre il quale la richiesta viene considerata non riuscita. In questo caso, la finestra temporale rimane disponibile per altre richieste.

Nota: la proprietà WorkFrameTimeout non viene controllata a meno che non sia richiesta una finestra temporale e tutte quelle definite siano già utilizzate. Pertanto, è abbastanza probabile che un server remoto abbia più tempo a disposizione di quello specificato dalla proprietà WorkFrameTimeout per rispondere. Il valore della proprietà WorkFrameTimeout è un valore minimo.

Questa proprietà è opzionale. Se omessa, il motore Web utilizza una finestra temporale di 30 secondi.

Capitolo 14: Utilizzo dell'API testo

Questa sezione contiene i seguenti argomenti:

API testo (a pagina 553)

API testo

L'*API testo* è un'interfaccia che consente di utilizzare l'input basato su testo per creare e aggiornare gli oggetti nel database CA SDM, come Issue, Richieste, contatti e asset. Utilizzando l'API testo è possibile assegnare dei valori alla maggior parte dei campi accessibili agli utenti.

Importante. CA SDM richiede che tutti i dati siano immessi in formato UTF-8, altrimenti possono essere danneggiati. L'utilità pdm_unconv (a pagina 1163) consente di convertire i dati di un set di caratteri da locale a UTF-8 e da UTF-8 a locale.

È possibile accedere all'API testo utilizzando le interfacce seguenti:

- Riga di comando
- Posta elettronica
- CA NSM

Nota: è possibile utilizzare i servizi Web in alternativa all'interfaccia API testo per l'integrazione tra più applicazioni.

Ulteriori informazioni:

Metodi di conversione (a pagina 565)

Interfaccia della riga di comando

Utilizzare il comando *pdm_text_cmd* per attivare l'interfaccia della riga di comando API di testo. Dopodiché è possibile immettere informazioni specifiche, ad esempio la tabella da elaborare e l'operazione da eseguire, utilizzando i parametri del comando pdm_text_cmd.

L'input dell'API testo viene passato al comando pdm_text_cmd nel formato file di input o direttamente da STDIN.

Nota: passando i parametri dal prompt dei comandi, utilizzare Ctrl+Z in Windows e Ctrl+D in POSIX.

Importante. Non è possibile utilizzare le virgolette singole o doppie come parametri per i comandi bop_cmd e pdm_text_nxd.

Ulteriori informazioni:

Interfaccia riga di comando di Text API - pdm_text_cmd (a pagina 1160)

Interfaccia di CA Network and Systems Management

Quando CA NSM e CA SDM vengono integrati e si creano le richieste da eventi di CA NSM, il parametro user_parms nelle definizioni delle regole dei writer viene passato all'interfaccia API testo. Il processo del writer di CA SDM (tngwriter) definisce i relativi parametri di sostituzione per la modifica del testo prima dell'invio all'interfaccia API testo. La parola chiave LOG_AGENT viene aggiunta in fondo all'input per impostare log_agent per la richiesta.

Nota: occorre aggiornare il fileText_API.cfg per tutti i campi aggiuntivi che vengono passati da Alert Management Systems CA NSM a CA SDM. Questo file è utilizzato per integrazioni con servizi Web, posta elettronica e AHD.DLL.

Ulteriori informazioni:

Parole chiave (a pagina 556)

Formato input

L'input dell'API testo è specificato nei seguenti modi:

- Nell'interfaccia riga di comando, l'input è normalmente specificato in un file di testo passato al comando pdm_text_cmd.
- Nell'interfaccia di posta elettronica, l'input è specificato nel testo del messaggio. Si specifica un'espressione regolare per individuare gli identificatori dell'oggetto di destinazione.

L'input di API testo si formatta allo stesso modo indipendentemente dall'interfaccia che si usa.

Il formato base dell'input è il seguente:

`%parola chiave=valore`

o

`%PROPERTY={{``etichetta_proprietà`**`}}`**`valore`

Il normale comportamento dei comandi API testo ha le seguenti eccezioni, in cui tra due o più comandi in conflitto tra loro, l'ultimo visualizzato ha precedenza:

- Quando un messaggio contiene più elementi di ID ticket corrispondenti alla stringa di filtro della regola di casella di posta, o più comandi ID ticket di API testo, viene utilizzato il primo riscontrato. Inoltre, un elemento di ID ticket, identificato mediante la stringa di filtro della casella di posta, sovrascrive qualsiasi comando ID ticket di API testo, indipendentemente da quale compare per primo.
- Quando un messaggio contiene più comandi API testo di commento del registro, tutti i commenti vengono pubblicati, anche se il loro ordine di apparizione nel registro delle attività di ticket può variare.

A tutti gli elementi di ID ticket corrispondenti al filtro, validi o meno, e i comandi ID ticket di API testo all'interno del messaggio, applicabili/applicati o meno, viene aggiunto un commento prima della pubblicazione del comando. Gli elementi di ID ticket identificati attraverso i filtri della regola della casella di posta vengono visualizzati come -((...))-. I segni di percentuale (%) nei comandi ID ticket di API testo vengono convertiti in due parentesi di apertura "((", e il comando è seguito da due parentesi di chiusura "))". Se un comando ID ticket di API testo compare dopo un altro comando API testo con un commento di registro (%LOG=...), il comando ID ticket di API testo viene trasformato in commento di registro separato.

Nota: il commento di registro è il solo comando API testo che può comparire più volte in un unico messaggio ed essere applicato a ogni occorrenza. Per tutti gli altri comandi, l'API testo utilizza solo l'ultima occorrenza, poiché le occorrenze multiple di altri comandi entrano in conflitto tra loro. I comandi di commento di registro multipli pubblicano messaggi di commento di registro separati e non necessariamente in un ordine definito.

Inoltre, se compare nel messaggio, all'inizio o tra altri due comandi API testo, un comando ID ticket di API testo viene convertito in commento di registro. Se il comando precedente è un commento di registro (%LOG=...) o una descrizione di aggiornamento (%DESCRIPTION=...), viene aggiunto a tale comando invece di essere trasformato in un commento di registro separato.

I messaggi in entrata inviati solo in formato HTML, senza inclusione della versione in testo normale, perdono il testo del messaggio. Se il messaggio corrisponde a qualsiasi filtro di regola di casella di posta elettronica con un testo vuoto, è possibile creare un ticket con una descrizione vuota o con l'oggetto del messaggio come intera descrizione del ticket.

Parole chiave

È possibile utilizzare due tipi di parole chiave come input per l'interfaccia API testo.

- Definizioni nella sezione [KEYWORDS] del file text_api.cfg — questo tipo è un gruppo di parole chiave che fa riferimento direttamente ai campi di varie tabelle aggiornabili. Ad esempio, la maggior parte dei campi del modulo Dettagli Issue sono definiti nella sezione [KEYWORDS]. Utilizzando queste parole chiave, è possibile impostare i valori per i campi nel record in fase di aggiornamento o creazione. Ad esempio, la riga seguente imposta la priorità della Issue su 5:

  ```
  %PRIORITY=5
  ```

  La sezione [KEYWORDS] del file text_api.cfg elenca tutte le parole chiave. È possibile definire parole chiave aggiuntive (ad esempio per consentire l'accesso dell'API testo ai campi aggiunti durante la personalizzazione dello schema del database).

- Le seguenti parole chiave speciali sono sempre definite come riportato qui, indipendentemente dai contenuti del file text_api.cfg:

Parola chiave	**Descrizione**
ASSET	Utilizzata per associare un elemento a un ticket. Questa parola chiave è valida per le Richieste, per le Issue e per gli Ordini di cambiamento. Il valore specificato è il nome dell'elemento, che deve essere già presente. È possibile specificare questa parola chiave più volte, poiché un ticket può essere associato più elementi.
ATTACHMENT	Utilizzata internamente dall'interfaccia di posta elettronica per aggiungere gli allegati di posta elettronica a un ticket.

Parola chiave	Descrizione
DESCRIZIONE	Specifica il valore da utilizzare per il campo della descrizione del ticket. Questa parola chiave viene utilizzata se l'input viene inviato all'interfaccia API testo senza una parola chiave esplicita. Questa parola chiave viene applicata automaticamente da Mail Eater quando il messaggio non inizia con una parola chiave ma contiene un elemento ID ticket o parola chiave. È possibile cambiare la modalità di gestione della parola chiave DESCRIPTION per gli aggiornamenti, utilizzando nella sezione [OPTIONS] del file text_api.cfg la voce seguente: UPDATE_DESC_IS_LOG Se questa opzione è impostata su YES, il valore viene utilizzato per creare un commento del registro. Se il valore è impostato su NO, il valore sovrascrive il valore esistente del campo della descrizione.
FROM_EMAIL FROM_EMAIL_OVERRIDE	Utilizzate dall'interfaccia di posta elettronica per eseguire l'associazione con il campo Indirizzo di posta elettronica nel record ca_contact. Viene utilizzato anche come log_agent per il ticket. Se entrambi sono forniti, FROM_EMAIL viene ignorato. **Nota:** FROM_EMAIL è impostato automaticamente da Mail Eater con l'indirizzo del mittente del messaggio.
FROM_PERSID	Utilizzata dall'interfaccia della riga di comando per definire log_agent per un'operazione. Ad esempio, quando un record ca_contact non dispone di ID utente. Questa parola chiave viene passata automaticamente da pdm_text_cmd se il parametro -p è specificato. Il valore viene associato a un persistent_id del record ca_contact.
FROM_USERID	Utilizzata solo nell'interfaccia della riga di comando per definire il comando log_agent per un'operazione. Questa parola chiave viene passata automaticamente da pdm_text_cmd se il parametro -u è specificato. Il valore viene associato a un ID utente di un contatto.
LOG	Utilizzata per creare una voce di registro. Questa parola chiave è valida per le Richieste, per gli Ordini di cambiamento, per le Issue e per i contatti. Questa parola chiave viene applicata automaticamente da Mail Eater quando il messaggio non inizia con una parola chiave ma contiene un elemento ID ticket o parola chiave, o una parola chiave DESCRIPTION.
LOG_AGENT	Utilizzata dall'interfaccia CA NSM per definire il comando log_agent per un'operazione. Il valore viene associato al campo ID di un record contatto.
PROPERTY	Utilizzata per impostare il valore di una proprietà. Questa parola chiave è valida solo per le Richieste, per gli Ordini di cambiamento e per le Issue. Contrariamente alle altre parole chiave, che sono seguite dal segno di uguale (=), la sintassi della parola chiave PROPERTY deve includere l'etichetta della proprietà, ad esempio: PROPERTY={{etichetta_proprietà}}valore È necessario specificare *etichetta_proprietà* esattamente come è riportata nel database.

Parola chiave	Descrizione
SEARCH	Utilizzata solo nell'interfaccia della riga di comando e nell'interfaccia CA NSM per fornire un elenco di parole chiave da utilizzare in una query per aggiornare più ticket di un asset. Il valore è un elenco di parole chiave da utilizzare nella ricerca. La parola chiave SEARCH viene impostata automaticamente dall'interfaccia CA NSM.
SEARCH_EXPLICIT	Utilizzata solo nell'interfaccia CA NSM in sostituzione della parola chiave SEARCH fornita dall'interfaccia CA NSM. I valori forniti sono uguali a quelli della parola chiave SEARCH.

Ulteriori informazioni:

Interfaccia riga di comando di Text API - pdm_text_cmd (a pagina 1160)

Convenzioni di immissione delle parole chiave

Al formato delle parole chiave immesse si applicano le seguenti convenzioni:

- Far precedere ogni parola chiave (inclusa PROPERTY) da un segno di percentuale (%). Il segno di percentuale deve essere in posizione colonna uno. Se la prima riga non vuota dell'input non contiene un segno di percentuale all'inizio della riga, viene utilizzato %DESCRIPTION= oppure %LOG= come prefisso per i dati in arrivo, a seconda che sia stato trovato un elemento ID ticket o una parola chiave. Se viene impostato %DESCRIPTION, il contenuto del messaggio fino alla prima parola chiave viene registrato come descrizione del ticket. Se viene impostato %LOG il contenuto del messaggio fino alla prima parola chiave viene registrato come commento registro.
- Non utilizzare spazi nella parola chiave, tra il segno di percentuale (%) e la parola chiave o tra la parola chiave e il segno di uguale (=).
- Non utilizzare le virgolette per i valori; tutti i dati dopo il segno = rappresentano il valore.
- La parole chiave non fanno distinzione tra maiuscole e minuscole.
- Se l'input include parole chiave duplicate, viene utilizzata l'ultima paraola chiave; altrimenti, l'ordine in cui vengono specificate le coppie parola chiave/valore è ininfluente.

- Specificare i valori della parola chiave come si farebbe per il campo corrispondente nell'interfaccia Web. Ad esempio, per specificare un tipo di contatto Analista, utilizzare %CONTACT_TYPE=Analista, anche se nel database questo valore viene memorizzato come valore intero. La parola chiave CONTACT_TYPE è definita nel file text_api.cfg, che converte il valore specificato (a pagina 565) in modo che corrisponda al valore memorizzato.

  Nota: il rispetto delle maiuscole/minuscole nel valore dipende dal DBMS utilizzato.

- I dati di tipo stringa possono occupare più righe.

Formattazione di un messaggio di posta elettronica per aggiornare un ticket

Un utente può formattare un messaggio di posta elettronica per creare o aggiornare un ticket.

Per formattare un messaggio di posta elettronica per creare o aggiornare un ticket, utilizzare i seguenti campi:

A

Specifica il nome della casella di posta assegnato al contatto CA SDM impostato per l'utente con privilegi.

Da

Specifica la persona che invia il messaggio di posta elettronica. La persona deve essere definita nella tabella ca_contact, a meno che nella regola della casella di posta applicabile non sia specificata l'opzione Consenti anonimo.

Nota: l'indirizzo Da fa tipicamente parte della configurazione del programma di posta elettronica in uso e non viene generalmente impostato a livello di messaggio.

Allegati

Consente di allegare documenti e altri file al messaggio di posta elettronica per inviare allegati all'interfaccia API testo.

Oggetto

Corrisponde a parole chiave di una stringa di filtro della regola della casella di posta, in particolare quando si crea un ticket.

Testo

Specifica il corpo del messaggio di posta elettronica utilizzando l'interfaccia API testo. È possibile specificare la parola chiave ISSUE_ID, REQUEST_ID o CHANGE_ID, in base al tipo di ticket, per creare o aggiornare un ticket.

Delimitatori di inizio e fine dei messaggi di posta elettronica

Alcune interfacce di posta elettronica aggiungono informazioni all'inizio o alla fine dei messaggi di posta elettronica (ad esempio la codifica MIME) che possono causare malfunzionamenti dell'interfaccia stessa. Se l'interfaccia di posta elettronica aggiunge informazioni, è possibile utilizzare i seguenti delimitatori: start-request ed end-request. L'interfaccia di posta elettronica ignora le informazioni che precedono il delimitatore start-request e che seguono il delimitatore end-request.

Nota: il daemon Mail Eater non supporta messaggi di posta elettronica in formato RTF o solo HTML.

Esempio: uso dei delimitatori start-request ed end-request

```
start-request
corpo_messaggio
end-request
```

Modalità di utilizzo degli elementi da parte dell'interfaccia API testo

L'interfaccia API testo elabora l'oggetto o il corpo del testo di notifiche di posta elettronica. Le regole della casella di posta consentono di identificare elementi e valori utilizzati dall'interfaccia API testo. Ad esempio, è possibile definire la regola per incidenti Incident:{{object_id}}, in modo che Incident:1234 venga tradotto in %INCIDENT_ID=1234 per l'interfaccia API testo, dove 1234 è il ref_num dell'incidente. Poiché nel messaggio di posta elettronica l'elemento deve essere univoco e facile da trovare, è possibile renderlo più distintivo, ad esempio %Incident:{{object_id}}%.

A questo scopo, apporre alla parola chiave {{object_id}} un carattere che non sia una lettera, un numero, una virgola, una barra (/) oppure un segno più (+) o uguale (=), poiché questi caratteri possono comparire all'interno di un elemento. In caso contrario, è possibile che i caratteri che seguono l'elemento vengano interpretati per una parte del valore dell'elemento oppure che un carattere all'interno del valore dell'elemento venga interpretato per un carattere che segue tale valore.

Il daemon Mail Eater esegue le operazioni riportate di seguito:

1. Trova l'elemento in un messaggio di posta elettronica (ad esempio, Incident:1234) che è associato al ticket appropriato o ad altro oggetto supportato dall'interfaccia API testo.
2. Traduce l'elemento in un token dell'interfaccia API testo (ad esempio, %INCIDENT_ID=1234).

3. Il daemon Mail Eater invia il messaggio con tag all'interfaccia API testo. L'interfaccia API testo elabora il messaggio di posta elettronica, applica il testo, i comandi o entrambi, che contiene nel ticket appropriato e genera una risposta automatica indicando se il messaggio di posta elettronica ricevuto è stato applicato correttamente. A seconda delle azioni eseguite, viene inoltre inviato un messaggio di posta elettronica separato per segnalare determinati eventi specifici, quali la creazione di un ticket.

Modalità di impostazione di risposte a notifiche di posta per l'aggiornamento di ticket

Il daemon API testo (pdm_text_nxd) crea e aggiorna ticket con informazioni provenienti da interfacce esterne, ad esempio la riga di comando e la posta elettronica. È possibile impostare la posta elettronica in modo che utilizzi l'interfaccia API testo per consentire agli utenti (contatti) di aggiornare ticket rispondendo a notifiche di posta elettronica. Il testo della risposta viene aggiunta al ticket come attività commento registro.

Per impostare risposte a notifiche per aggiornare ticket, procedere come segue:

1. Impostare il metodo di notifica utilizzato dal contatto su pdm_mail –T *indirizzo_postal_risposta* o su pdm_mail –F *indirizzo_postal_risposta.* L'*indirizzo_postal_risposta* specifica l'indirizzo della posta elettronica in entrata della casella di posta. Quando il contatto fa clic su Rispondi nel messaggio di posta elettronica, l'indirizzo viene compilato dall'indirizzo Da o Rispondi a del messaggi al quale sta rispondendo.

   -T imposta l'indirizzo Rispondi a. -F imposta l'indirizzo Da, che è utilizzato come indirizzo di risposta se non ne viene specificato un altro.

   Nota: alcuni programmi di posta elettronica non usano o non possano utilizzare l'indirizzo Rispondi a.

2. Creare o aggiornare una regola della casella posta utilizzando una password dell'interfaccia API testo.

   Gli elementi definiti dall'utente nei filtri della regola della casella di posta sostituiscono le seguenti parole chiave dell'interfaccia API testo:

Oggetto	Parola chiave API testo	Identificativo
Incidente	%INCIDENT_ID	Ref_num
Problema	%PROBLEM_ID	Ref_num
Richiesta	%REQUEST_ID	Ref_num
Chg_ref_num	%CHANGE_ID	Chg_ref_num
Issue	%ISSUE_ID	Ref_num

3. Creare o aggiornare una frase di notifica che corrisponde alla regola.
4. Creare o aggiornare un modello di messaggio che utilizza la frase di notifica.
5. Aggiornare la regola della casella di posta creata nel passaggio 2 per specificare il modello di messaggio che è stato creato o aggiornato nel passaggio 4.

Nota: per informazioni sull'esecuzione di ogni passaggio, consultare la *Guida in linea*.

Dopo che l'utente riceve la notifica e risponde, si verificano le seguenti azioni:

1. Quando viene trovata la stringa di filtro, l'eventuale parola chiave e il valore dell'ID ticket denotati dal segnaposto vengono aggiunti al messaggio.
2. Se viene trovato un elemento ID ticket corrispondente, il ticket corrispondente viene aggiornato con un commento registro o una nuova descrizione o altri valori in base al testo, alle parole chiave e ai comandi nel messaggio.
3. Se non viene trovato un elemento ID ticket corrispondente, viene creato un ticket con una descrizione e altri parametri in base al testo, alle parole chiave e ai comandi nel messaggio.

Esempio di impostazione di una risposta a una notifica di incidente

L'esempio riportato di seguito illustra come impostare una risposta a una notifica di incidente.

Per impostare una risposta a una notifica di incidente, procedere come segue:

1. Creare una regola della casella di posta utilizzando i seguenti campi e valori:
   - Filtro—Corpo del messaggio contiene
   - Stringa filtro—%Incident:{{object_id}}%
   - Ignora maiuscole/minuscole—SÌ
   - Azione—Aggiorna oggetto
   - Oggetto azione—Incidente
2. Creare un frase di notifica che includa la regola, come illustrato di seguito:
   - Simbolo—Risposta incidente
   - Codice—IncidentReply

- Attivo—Attivo
- Descrizione—Commento che incorpora la risposta a un incidente/problema/richiesta.
- Frase—Per aggiungere un commento a @{call_req_id.type.sym}, è sufficiente rispondere a questo messaggio di posta elettronica o includere la riga seguente (in una riga autonoma):

  ```
  %Incident:{call_req_id.ref_num}%
  ```

  Nota: nel testo di risposta automatica delle regola della casella di posta, omettere il prefisso call_req_id . Questo prefisso applica un contesto in cui il testo della regola della casella di posta si trova già e tale modifica di contesto non è valida quando si opera già da tale contesto.

3. Creare o aggiornare un modello di messaggio che utilizza la frase di notifica come indicato di seguito:

   - Testo del messaggio di notifica

     ```
     Questa è una semplice notifica.
     @{notification_phrase[IncidentURL1].phrase}
     ```

4. Aggiornare la regola della casella di posta creata nel passaggio 1 per specificare il modello di messaggio che è stato creato nel passaggio 3, come indicato di seguito:

   Modello messaggio—*nome della regola della casella di posta*

Modalità di aggiornamento di un esempio di ticket da parte di un utente finale

L'esempio riportato di seguito dimostra come un utente finale (John Smith) risponde a una notifica di posta elettronica per aggiornare un ticket incidente.

Il corpo o l'oggetto del messaggio include l'identificativo dell'oggetto. Il segnaposto {{object_id}} all'interno della stringa di filtro denota l'identificativo dell'oggetto.

1. Viene inviata una notifica a John Smith che include le seguenti istruzioni:

   ```
   Per aggiungere un commento all'incidente, è sufficiente rispondere a questo messaggio di posta elettronica o includere la riga seguente (in una riga autonoma).
   %Incident:1234%
   ```

2. John Smith risponde alla notifica come segue:

   ```
   Questa è la mia risposta...
   ```

3. Il daemon Mail Eater riceve la seguente versione di testo del messaggio di John Smith:

```
Questa è la mia risposta...

Da: Service Desk
Inviato: mercoledì 18 settembre 2009 10:22
A: Smith, John
Oggetto: Semplice notifica

Questa è una semplice notifica.

Per aggiungere un commento all'incidente, è sufficiente rispondere a questo
messaggio di posta elettronica o includere la riga seguente (in una riga autonoma).

%Incident:1234%
```

4. Il daemon Mail Eater elabora le regole nell'ordine e trova l'elemento %Incident:1234%:

```
Questa è la mia risposta...

Da: Service Desk
Inviato: mercoledì 18 settembre 2009 10:22
A: Smith, John
Oggetto: Semplice notifica

Questa è una semplice notifica.

Per aggiungere un commento all'incidente, è sufficiente rispondere a questo
messaggio di posta elettronica o includere la riga seguente (in una riga autonoma).
%INCIDENT_ID=1234
```

5. Il daemon Mail Eater aggiunge le parole chiave dell'interfaccia API testo e il valore {{object_id}} a un'istruzione %INCIDENT_ID= e lascia un marcatore dove è stato trovato il valore {{object_id}}. Il testo seguente mostra i dai inviati all'interfaccia API testo. Il testo in grassetto indica i valori aggiunti dal daemon Mail Eater.

```
%LOG=Questa è la mia risposta...
Da: Service Desk
Inviato: mercoledì 18 settembre 2009 10:22
A: Smith, John
Oggetto: Semplice notifica

Questa è una semplice notifica.

Per aggiungere un commento all'incidente, è sufficiente rispondere a questo
messaggio di posta elettronica o includere la riga seguente (in una riga autonoma).
%Incident:-((...))-%
%FROM_EMAIL=john.smith@azienda.com
%INCIDENT_ID=1234
```

6. L'interfaccia API testo aggiunge un commento registro per l'Incidente 1234.

Metodi di conversione

A molte delle parole chiave definite nel file text_api.cfg è associato un metodo per convertire il valore specificato in un valore appropriato per la memorizzazione nel database. Questa funzione consente agli utenti di specificare i valori come nell'interfaccia Web, senza dover conoscere il tipo di implementazione di base.

Il file di configurazione include diversi esempi di questo tipo di definizione delle parole chiave tra cui ISSUE.PRIORITY e CONTACT.CONTACT_TYPE. Se è necessario definire parole chiave aggiuntive, ad esempio per consentire l'accesso dell'API testo ai campi aggiunti durante la personalizzazione dello schema del database, è possibile utilizzare uno dei seguenti metodi predefiniti:

Metodo	**Tipo di output**
lookup_actbool	INTEGER
lookup_asset_by_name	UUID
lookup_asset_by_persid	UUID
lookup_chg_category	STRING
lookup_chg_status	STRING
lookup_cnt_by_email	UUID
lookup_cnt_by_last_first_middle	UUID
lookup_cnt_by_logonid	UUID
lookup_cnt_by_persid	UUID
lookup_cnt_meth	INTEGER
lookup_cnt_type	INTEGER
lookup_company	UUID
lookup_cr_status	STRING
lookup_cr_template	STRING
lookup_domain	INTEGER
lookup_grc	INTEGER
lookup_group	UUID
lookup_impact	INTEGER
lookup_iss_category	STRING
lookup_iss_status	STRING
lookup_loc	UUID

Metodo	Tipo di output
lookup_mfr_model	UUID
lookup_nr_family	INTEGER
lookup_org	UUID
lookup_person_contacting	INTEGER
lookup_position	INTEGER
lookup_priority	INTEGER
lookup_prob_category	STRING
lookup_product	INTEGER
lookup_resource_status	INTEGER
lookup_service_lvl	STRING
lookup_severity	INTEGER
lookup_state	INTEGER
lookup_timezone	STRING
lookup_type_of_contact	INTEGER
lookup_urgency	INTEGER
lookup_workshift	STRING

Se il valore da convertire non è supportato da nessuno dei metodi predefiniti, è necessario creare un metodo personalizzato. Il metodo dovrebbe utilizzare un valore STRING come input e restituire come output un valore INTEGER, STRING o UUID. La restituzione di un valore -1 (o "-1") indica che il valore non può essere determinato e quindi non impostato. Per UUID, il valore restituito deve essere "(uuid) NULL".

Ad esempio, è possibile sviluppare un metodo per convertire un ID utente in un riferimento di tabella ca_contact. Il valore di input, ad esempio Amministratore, verrebbe passato al metodo e il metodo dovrebbe restituire l'ID della tabella ca_contact per l'ID utente dell'amministratore.

Il modo con cui si definiscono le parole chiave nel file di configurazione consente di definire più associazioni di parole chiave nello stesso campo, inclusi diversi metodi di conversione, in base al valore specificato. Ad esempio, è possibile che per l'assegnatario vi siano differenti associazioni di parole chiave per definire in che modo impostare il valore in base a differenti valori di input. Un input potrebbe essere l'ID utente e un altro potrebbe essere il cognome, il nome, il secondo nome e un altro ancora potrebbe essere l'ID ca_contact effettivo, ad esempio 793ED69B4E87A545BD8E911834D829FC). Ogni parola chiave viene associata a un metodo di conversione differente, tranne l'ultima che non deve essere convertita.

File di configurazione

Il file text_api.cfg definisce le parole chiave direttamente correlate ai campi di varie tabelle che è possibile aggiornare. Questo file verrà utilizzato sia come riferimento per trovare valori predefiniti specifici, ad esempio le parole chiave, sia come meccanismo per la configurazione dell'API testo, sebbene il file di configurazione predefinito possa essere utilizzato nella maggior parte delle installazioni senza dovervi apportare alcuna modifica.

Il file text_api.cfg si trova nella directory seguente:

- UNIX—$NX_ROOT/site
- Windows—*installation-directory*\site. Ad esempio: C:\Program Files\CA\Service Desk\site

Il file di configurazione è diviso in sezioni e in ognuna di esse sono definiti attributi specifici. Le definizioni degli attributi sono nel formato seguente:

```
parola chiave=valore
```

Contrariamente a tutti gli altri valori, le parole chiave non rispettano l'uso delle maiuscole/minuscole, ad eccezione della sezione [OPTIONS].

Nota: il file text_api.cfg può essere modificato mediante qualsiasi editor di testo.

Importante. Se si sta eseguendo l'integrazione con il componente CA NSM Alert Management Systems, è necessario aggiornare text_api.cfg per qualsiasi campo aggiuntivo passato a CA SDM.

Ulteriori informazioni:

Parole chiave (a pagina 556)

Opzioni

La sezione [OPTIONS] del file text_api.cfg definisce le opzioni di elaborazione che potrebbero essere differenti da un sito all'altro. Ad esempio, sono disponibili opzioni per determinare il formato della data di input, per indicare i campi che consentono il mantenimento degli avanzamenti di riga e opzioni che consentono di specificare se consentire l'aggiornamento delle questioni, delle richieste o degli ordini di cambiamento utilizzando l'interfaccia di posta elettronica. Tutte le opzioni di questa sezione sono configurabili. Tenere presente che, sebbene sia possibile rimuovere i nomi di tabella dall'elenco VALID_TABLE_LIST, se non si desidera supportare l'accesso dell'interfaccia API testo a queste tabelle, è possibile non aggiungere i nomi di tabella a tale elenco.

Impostazioni predefinite

Utilizzare la sezione [XX_DEFAULTS] del file text_api.cfg per ciascuna interfaccia utilizzando l'Api di testo (ad esempio, [EMAIL_DEFAULTS] per l'interfaccia di posta elettronica e [CMD_DEFAULTS] per l'Interfaccia della riga di comando). La sezione [XX_DEFAULTS] definisce i valori predefiniti per i campi e le proprietà richieste nel caso in cui non vengano specificati dall'utente. XX fa riferimento al tipo di interfaccia, ad esempio CMD o EMAIL.

Per impostare i valori predefiniti, utilizzare uno dei formati seguenti:

- nome_tabella**.**parola chiave**=**valore

  La *parola chiave* deve essere definita nella sezione [KEYWORDS] oppure come proprietà nel database. Qualsiasi metodo associato alla parola chiave viene automaticamente applicato al *valore*. Ad esempio:

  ```
  ISSUE.PRIORITY=1
  ```

  La parola chiave PRIORITY viene definita nel file text_api.cfg in modo che esegua una ricerca per convertire il valore specificato affinché corrisponda al relativo valore memorizzato nel database. In questo esempio il valore 1 viene convertito in 5, ovvero nel valore del database di base per il simbolo della priorità 1. Questa funzione consente agli utenti di specificare lo stesso valore che si immetterebbe nell'interfaccia Web.

- nome_tabella**.PROPERTY={{**etichetta_proprietà**}}**valore

  L'*etichetta_proprietà* deve essere definita nel database come una proprietà.

In entrambi i formati, *nome_tabella* deve essere uno dei valori definiti da VALID_TABLE_LIST nella sezione [OPTIONS], ad esempio Questione, Richiesta o Contatto.

Ulteriori informazioni:

Metodi di conversione (a pagina 565)

Sezione Ignore Incoming

Sono presenti diverse sezioni [..._IGNORE_INCOMING] nel file text_api.cfg file, una per ogni interfaccia che utilizza API testo, ad esempio la sezione [TNG_IGNORE_INCOMING] per l'interfaccia CA NSM e la sezione [EXT_IGNORE_INCOMING] per l'interfaccia esterna utilizzata da altri prodotti CA. Queste sezioni definiscono i campi e le proprietà ignorati nell'input. Il formato è uguale a quello descritto per la sezione DEFAULT ma "**=***valore*" non viene specificato. Ciò consente di evitare che gli utenti impostino determinati valori, il che garantisce maggiore sicurezza in determinate circostanze, come quando si consente ai clienti di usare l'interfaccia di posta elettronica.

Le sezioni IGNORE funzionano al meglio quando utilizzate insieme alle sezioni [..._DEFAULTS] corrispondenti, poiché impediscono agli utenti di impostare un determinato valore e allo stesso tempo forniscono un valore predefinito. Ad esempio, per impedire agli utenti dell'interfaccia di posta elettronica di impostare i valori di priorità di una questione, è possibile specificare i valori seguenti:

```
[EMAIL_DEFAULTS]
ISSUE.PRIORITY=2
[EMAIL_IGNORE_INCOMING]
ISSUE.PRIORITY
```

In questo caso, qualsiasi valore di priorità specificato dall'utente nel corpo del messaggio di posta elettronica viene ignorato e a tutte le questioni create dall'interfaccia di posta elettronica viene automaticamente assegnata la priorità 2.

Input di esempio

Gli esempi seguenti mostrano l'input da utilizzare nel testo di un messaggio di posta elettronica o in un file che funge da input per l'interfaccia della riga di comando.

Esempio: la prima riga non contiene una parola chiave

In questo esempio, dal momento che nella prima colonna della prima riga manca il parametro %keyword, la stringa %DESCRIPTION= viene aggiunta all'inizio del messaggio. In questo modo, il valore del campo della descrizione è "Questo testo viene inserito nel campo descrizione". La descrizione include l'interruzione di riga, poiché il parametro ISSUE.DESCRIPTION è incluso nell'elenco dei campi dell'elemento LINEFEEDS_ALLOWED nella sezione [OPTIONS] del file text_api.cfg.

```
Questo testo viene inserito
nel campo descrizione
%PRIORITY=Nessuna
```

Esempio: la prima riga contiene una parola chiave

In questo esempio, la parola chiave PRIORITY viene definita nel file text_api.cfg in modo che esegua una ricerca per convertire il valore specificato affinché corrisponda al relativo valore memorizzato nel database. In questo esempio il valore Nessuno viene convertito in 0, ovvero nel valore del database di base per il simbolo della priorità 1. Questa funzione consente agli utenti di specificare lo stesso valore che si immette nell'interfaccia Web.

```
%description=Questa è la mia descrizione
%priority=Nessuna
%CATEGORY=Aggiornamento.PC
%PROPERTY={{CPU corrente}}266 MHz
%PROPERTY={{Disco rigido corrente}}1 GB
%PROPERTY={{Aggiornamento richiesto}}4 GB di disco rigido
```

I valori specificati vengono utilizzati per impostare i campi descrizione e priorità per il ticket, analogamente all'esempio precedente. Tenere presente che per la parola chiave l'uso delle maiuscole e delle minuscole non è rilevante.

Viene ricercato il valore di Aggiornamento.PC e il campo categoria del ticket viene impostato nel modo appropriato.

L'associazione delle etichette seguenti imposta i valori delle tre proprietà:

- CPU corrente
- Disco rigido corrente
- Aggiornamento richiesto

Capitolo 15: Controllo delle versioni per le personalizzazioni di sistema nei vari server di CA SDM

Il controllo versioni di CA SDM consente di gestire le personalizzazioni di sistema su tutti i server di CA SDM (client e server). In base alla configurazione di CA SDM, vengono utilizzati i client e i server seguenti:

- Configurazione convenzionale
  - Client: server secondario
  - Server: server primario
- Configurazione con disponibilità avanzata
  - Client: server applicazioni e server di standby
  - Server: server in background

Esempio: In qualità di amministratori di sistema, si è aggiunto un campo nella pagina detail_usp_server.htmpl di CA SDM. Ora si desidera sincronizzare questa modifica sui vari client e server. Questo esempio viene utilizzato nello scenario per spiegare le modalità con cui la personalizzazione viene sincronizzata.

Il diagramma seguente mostra la procedura per il controllo delle versioni delle personalizzazioni di sistema sui server di CA SDM:

Procedere come descritto di seguito:

1. Verificare i prerequisiti (a pagina 572).
2. Apportare modifiche in CA SDM. In questo esempio, aggiungere il nuovo campo nella pagina HTMPL di CA SDM.
3. Modificare il file di controllo versioni del server (a pagina 573).
4. Riavviare CA SDM sul client.
5. Verificare le personalizzazioni sul client (a pagina 580).

Verifica dei prerequisiti

Verificare i seguenti prerequisiti:

- Controllare che l'opzione ver_ctl sia impostata sul valore di **aggiornamento**. Quando si rileva una differenza di versione, sul client si tenta l'aggiornamento dei componenti interessati. Se l'aggiornamento riesce, la connessione client con il server continua, altrimenti la connessione viene chiusa. Per ulteriori informazioni sull'opzione ver_ctl, consultare la *Guida in linea*.

- Controllare che il file server_secondary_custom.ver sia creato nella directory $NX_ROOT\site\mods del server primario o del server in background, a seconda della configurazione di CA SDM. Tutte le personalizzazioni di un componente di controllo versioni devono essere eseguite in questo file. Se il file non esiste, crearlo nella stessa posizione.

Modifica del file di controllo versioni del server

Dopo aver completato la personalizzazione (ad esempio, è stato aggiunto un campo nella pagina HTMPL), aggiungere o aggiornare i componenti del controllo versioni sul file di controllo versioni del server. Un componente del controllo versioni può rappresentare un file, una directory o il file delle variabili di ambiente client_nx.env.

Procedere come descritto di seguito:

1. Accedere al server seguente, a seconda della configurazione di CA SDM:
   - Convenzionale: server primario
   - Disponibilità avanzata: server in background
2. Accedere alla seguente directory:

   `$NX_ROOT\site\mods`
3. Aprire il file server_secondary_custom.ver.
4. Aggiungere i componenti seguenti:

   ```
   [ MY_USP_SERVERS_HTMPL ]
   directory="$NX_ROOT/site/mods/www/htmpl/web/analyst/Analyst"
   filename="detail_usp_servers.htmpl"
   version="2.0 , 20121119"
   o_mode="RW"
   g_mode="RW"
   w_mode="RW"
   file_ctl
   ```

   Nota: Per ulteriori informazioni sull'aggiunta o sull'aggiornamento dei componenti di controllo versioni, consultare l'argomento Componenti di controllo versioni (a pagina 574).
5. Salvare il file server_secondary_custom.ver.

   Il componente di controllo versioni è stato aggiunto al file di controllo versioni.

Componenti di controllo versioni

Per definire un nuovo componente,

- utilizzare la seguente sintassi. Le voci in *corsivo* rappresentano i dati specificati dall'utente. I parametri *nome-componente* e versione sono obbligatori. Altri parametri potrebbero essere obbligatori, in base al valore *tipo-controllo*. Tutti gli altri elementi rappresentano parole chiave che è necessario immettere esattamente come nel seguente esempio:

```
[ nome componente ]

version = "x.x, ddmmyyyy"

tipo-controllo

filename = "nomefile"

directory = "directory"

link = "directory-collegamento"

source = "directory-origine"

effectivity = "spec-efficacia"

checksum

min_release = "release"

max_release = "release"

component_type = "tipo-file"

o_mode = "modalità-proprietario"

g_mode = "modalità-gruppo"

w_mode = "modalità globale"
```

Nota: Per ulteriori informazioni sui parametri, consultare l'argomento Parametri di controllo versioni (a pagina 575). Per ulteriori informazioni sulla struttura e sulla sintassi dei file di controllo versioni, consultare i file .ver installati nella directory $NX_ROOT\site. Questi file contengono commenti e impostazioni di esempio che possono risultare utili.

Per aggiornare una voce di componente esistente,

- Modificare il parametro. Ad esempio, modificare il numero di versione.

Per rimuovere un controllo da un componente,

- Modificare il componente secondo la procedura descritta:

```
! uncontrol nome-componente
```

Parametri del servizio Controllo versione

I parametri seguenti sono validi per il servizio Controllo versione:

[nome componente]

Specifica il nome di un elemento nel servizio Controllo versione. Il nome deve essere univoco ed essere racchiuso tra parentesi quadrate. *nome componente* non è sensibile alle maiuscole. Questo parametro è necessario per iniziare la definizione di un componente.

version="x.x. yyymmd"

Specifica un numero di versione (*x.x*) e una data (*ddmmyyyy*) che definiscono la versione del componente. Questo parametro è obbligatorio e deve essere racchiuso tra virgolette. Il servizio Controllo versione verifica la versione di un componente confrontando il numero di versione e la data sul server con il numero di versione e la data sul client. I numeri di versione e le date devono corrispondere affinché il componente possa essere considerato sincronizzato tra il client e il server. Opzionalmente, se la proprietà checksum è abilitata, prima di essere aggiornato, il file viene verificato in base a tale proprietà.

tipo-controllo

Specifica il tipo di versione del componente. Per tipo-controllo sono valide le seguenti impostazioni:

Impostazione	Descrizione
dir_ctl	Specifica che il componente rappresenta una directory. È necessario fornire il parametro directory per specificare il percorso alla directory. È possibile fornire anche il parametro di nome del file per filtrare un insieme di file nella directory. Le sottodirectory non vengono aggiornate in UNIX o in Windows.
file_ctl	Specifica che il componente rappresenta un file. È necessario fornire il parametro filename per specificare il percorso al file.
Nxenv_ctl	Specifica che il componente rappresenta il file client_nx.env, utilizzato per memorizzare le variabili di ambiente interne di CA SDM. Il controllo versioni di CA SDM e Gestione Opzioni gestiscono automaticamente questo file. È presente un solo componente nxenv_ctl e il suo nome deve essere CLIENT_NXENV.

Impostazione	Descrizione
ver_ctl	Si tratta del tipo di controllo predefinito. Specifica che il componente è generico, ovvero, non è associato a nessun oggetto esterno specifico. È possibile utilizzare un componente generico per eseguire il controllo della versione del client oppure di un file o di una directory le cui dimensioni sono eccessive per un aggiornamento automatico. I componenti con un tipo di controllo ver_ctl non possono essere aggiornati; in caso di mancata corrispondenza di versione in un componente ver_ctl quando il server è in modalità AGGIORNAMENTO, si verifica un errore di connessione del client.

filename="nomefile"

Specifica il nome di un file in Controllo versione. Non contiene specifiche di directory. Questo parametro è obbligatorio per i componenti file_ctl ma è opzionale per i componenti di controllo directory (dir_ctl). Quando utilizzato con i componenti directory, il parametro filename agisce come un filtro file per limitare i file associati al componente dir_ctl. Ad esempio, se il parametro filename per un componente dir_ctl è *.README, un aggiornamento da tale directory include solo i file il cui nome termina con “.README.”.

directory="directory"

Specifica il percorso alla directory dei componenti dir_ctl oppure alla directory contenente il file dei componenti file_ctl. Questo parametro viene ignorato per i componenti ver_ctl e nxenv_ctl. Il percorso alla directory deve essere racchiuso tra virgolette e può contenere i riferimenti alle variabili di ambiente preceduti dal simbolo $.

Nota: per separare le sottodirectory, nel percorso utilizzare sempre le barre (/) e non le barre rovesciate (\), questa indicazione è valida anche per il server Windows.

link="directory-collegamento"

Specifica una directory di collegamento sul client nello stesso formato precedentemente descritto per il parametro directory. Questo parametro è opzionale per i componenti file_ctl e dir_ctl e viene ignorato per i componenti ver_ctl e nxenv_ctl. Se specificato, l'aggiornamento a un client Linux causa il posizionamento nella directory di collegamento di un collegamento simbolico che punta al file effettivo copiato nell'ubicazione specificata dal parametro directory. Se si aggiorna un client Windows, il file effettivo viene copiato nella posizione del parametro link e nella posizione del parametro directory.

source="directory-origine"

(Opzionale) Specifica una directory differente sul server in cui il server può recuperare i file per la distribuzione. Questo parametro ha lo stesso formato precedentemente descritto per il parametro directory. È utile se i file da consegnare al client sono differenti rispetto agli stessi file presenti nella directory del server. Questo parametro viene utilizzato per indicare al server di recuperare il file dalla *directory-fonte* e distribuirlo nella posizione del client specificata dal parametro directory. Il parametro directory è obbligatorio se si specifica il parametro source.

effectivity="spec-efficacia"

(Opzionale) Specifica se il client deve acquisire il componente. Consente di escludere il download in determinati client. Se un client è escluso dalla specifica del parametro effectivity, non può acquisire il componente. Se questo parametro viene omesso, tutti i client ricevono il componente. Per questo parametro vengono utilizzati i simboli seguenti:

+ (segno più)

Indica di aggiungere un gruppo di client.

- (segno meno)

Indica di escludere un gruppo di client.

Sono validi i seguenti gruppi di client:

- SUN4SOL
- AIX
- LINUX
- LINUX390
- HP
- WINDOWS_CLIENTS
- UNIX_CLIENTS

Ad esempio, la specifica seguente indica che solo i client UNIX acquisiscono i file:

```
effectivity = "+ UNIX_CLIENTS"
```

checksum

Indica al componente di eseguire l'aggiornamento se il checksum del componente sul client non corrisponde al relativo checksum sul server. Se applicato a una directory, il checksum viene applicato a ogni file.

min_release="release" e max_release="release"

Specifica il client meno recente e quello più recente a cui dovrebbe essere distribuito il componente. Le istruzioni nel file server_default.ver definiscono le release. Questi parametri sono nel formato illustrato di seguito, dove Ga*xx* indica la release e i valori successivi sono i livelli generali associati alla release.

```
! Release GA50 50MVV000900 50W7T000900
! Release GA45 45MW000900 50WTT000900
```

L'ordine indica che GA50 è più recente di GA45.

component_type

Specifica il tipo di componente utilizzato. Vengono utilizzati i seguenti tipi di componenti:

Impostazione	Descrizione
file	Si tratta del tipo di componente predefinito. Specifica che i file copiati sul client sono ottenuti direttamente dall'ubicazione del server indicata dal parametro directory.
exe_file	Specifica che i file copiati sul client sono ottenuti da una posizione del server dipendente dal sistema operativo del client, come mostrato di seguito: ■ windows (Windows) ■ sun4Sol (Solaris) ■ hp (HP-UX) ■ aix (AIX) ■ linux (Linux) ■ linux390 (Linux390) Le posizioni di queste sottodirectory dipendono dall'impostazione del parametro directory. Se questo parametro è impostato, le sottodirectory si trovano nella *directory* indicata. In caso contrario, si trovano nella directory bin della directory di installazione principale di CA SDM.

o_mode="modalità-proprietario"

Specifica le autorizzazioni di accesso al file per il proprietario del file.

g_mode="modalità-gruppo"

Specifica le autorizzazioni di accesso file per gli utenti presenti nel gruppo del proprietario del file (solo per i client UNIX).

w_mode="modalità-globale"

Specifica le autorizzazioni di accesso file per gli utenti non compresi nel gruppo del proprietario del file (solo per i client UNIX).

I tre parametri mode consentono la gestione sul server di versioni differenti dello stesso file eseguibile. Specificano i controlli per l'accesso al file quando viene copiato sul client. Questi parametri vengono utilizzati solo durante un'operazione di aggiornamento. Sono costituiti da uno a tre caratteri, con il significato seguente:

Impostazione	Descrizione
R	Lettura
W	Scrittura
X	Esegui

I client PC ignorano le autorizzazioni di tipo Scrittura ed Esecuzione.

È possibile specificare una combinazione qualsiasi composta da una o più modalità di accesso file. Sui client UNIX, al file viene assegnata la modalità di accesso specificata. Sui client PC, il file è in modalità di scrittura o sola lettura, in base a come è stato specificato il parametro w_mode.

Riavvio di CA SDM sul client

CA SDM viene riavviato sui server client per aggiornare i file di controllo versioni del client con le personalizzazioni.

Nota: Selezionare Start, Impostazioni, Pannello di controllo, Strumenti di amministrazione, Servizi. Fare clic con il pulsante destro del mouse sul server di CA SDM e selezionare Inizio per riavviare o avviare un server.

Procedere come descritto di seguito:

1. Per la configurazione convenzionale, riavviare il server secondario.
2. Per la configurazione con disponibilità avanzata, completare i passaggi seguenti:
    a. Riavviare tutti i server di standby.
    b. Scegliere il server applicazioni meno attivo (a pagina 36).
    c. Riavviare il server applicazioni meno attivo.
    d. Arrestare l'altro server applicazioni (a pagina 37).
    e. Avviare il server applicazioni.
    f. Eseguire i passaggi d ed e per più server applicazioni.

    Il client si connette al server per inviare un elenco dei componenti controllati. Il server confronta l'elenco con il proprio elenco principale. I componenti interessati sul client sono stati aggiornati.

Scegliere il server applicazioni meno attivo

Scegliere un server applicazioni con l'attività utente più bassa. Eseguire il comando seguente su ciascun server applicazioni per scegliere quello con il numero più basso di sessioni attive o con nessuna sessione attiva.

```
pdm_webstat
```

Nota: Questo comando non acquisisce le sessioni SOAP o del servizio Web REST.

Arresto dell'altro server applicazioni

Tutti gli utenti attivi su un server applicazioni vengono informati di spostarsi sul server applicazioni meno attivo prima di arrestarlo. Assicurarsi di avere riavviato il server applicazioni meno attivo prima di spostare tutti gli utenti su di esso.

Procedere come descritto di seguito:

1. (Consigliato) Informare tutti gli analisti di Support Automation attivi sul server applicazioni che si desidera arrestare di creare un ticket in CA SDM con le informazioni sulla sessione. Questo processo assicura che le informazioni sulla sessione non vengano perse. Ad esempio, l'analista di Support Automation si trova in una sessione con un cliente per risolvere un problema di hardware. In tale caso, l'analista di Support Automation può creare un problema in CA SDM con le informazioni sulla sessione prima che il server applicazioni venga arrestato.
2. Inviare una notifica (ad esempio, una notifica di posta elettronica) a tutti gli utenti attivi sul server applicazioni perché si spostino sul server applicazioni meno attivo che è stato appena riavviato. Questa notifica può includere i dettagli del server applicazioni aggiornato.
3. Eseguire il comando seguente sul server applicazioni:

   ```
   pdm_server_control [-h] -q interval -s server_name
   ```

   -h

   Visualizza la pagina della Guida.

   -q interval -s server_name

   Notifica a un server applicazioni locale o remoto di rimanere inattivo in un intervallo di tempo specificato. Questo intervallo è il numero di secondi prima che il server diventi non in linea. Quando si utilizza questa opzione senza un server_name, il server locale viene informato di rimanere inattivo. Non è possibile utilizzare questa opzione per un server in background o di standby.

   Tutti gli utenti attivi sul server applicazioni visualizzano un messaggio popup che li informa dell'arresto del server e del tempo rimasto prima dell'arresto. Gli utenti devono salvare il proprio lavoro e uscire entro il tempo indicato. Il server applicazioni si arresta dopo il tempo specificato. Gli utenti accedono all'altro server applicazioni per riprendere il lavoro. L'analista di Support Automation può fare riferimento al ticket e riprendere il lavoro.

   L'arresto del server applicazioni è riuscito.

Verifica delle personalizzazioni sul client

Il file di controllo versioni viene verificato sul client per controllare se tutte le personalizzazioni sono state sincronizzate.

Procedere come descritto di seguito:

1. Accedere al client seguente, a seconda della configurazione di CA SDM:
   - Convenzionale: server secondario
   - Disponibilità avanzata: server di standby e server applicazioni
2. Aprire il file stdlog dalla posizione seguente:

   `$NX_ROOT\log`

3. Controllare se tutte le personalizzazioni effettuate sul server siano applicate sul client.

Capitolo 16: Gestione degli elementi di configurazione

Questa sezione contiene i seguenti argomenti:

Utilizzo dell'interfaccia Web (a pagina 583)
Contatto, posizione ed elementi della configurazione dell'organizzazione (a pagina 588)
Relazioni elemento della configurazione (a pagina 592)
Controllo delle versioni (a pagina 601)
Visualizzazione degli attributi degli elementi della configurazione in altri prodotti CA (a pagina 633)
Utilizzo di Visualizzatore CMDBf (a pagina 634)
Visualizzatore CMDB (a pagina 634)
Aggiunta di un asset rilevato (a pagina 638)
Flag di asset ed elementi della configurazione (a pagina 639)
Riconciliazione elementi della configurazione (a pagina 640)
Gestione di transazioni con installazione di appoggio (a pagina 663)
Manutenzione dei dati di CA CMDB (a pagina 688)
Funzionalità CACF (Configuration Audit and Control Facility) (a pagina 703)

Utilizzo dell'interfaccia Web

A seconda del proprio ruolo, è possibile eseguire attività di utente e amministrazione relativamente ai seguenti elementi della configurazione:

- I contatori consentono di eseguire attività di utente e gestire elementi della configurazione e relazioni tra gli stessi.
- La scheda Amministrazione consente di eseguire attività di amministrazione con gli elementi della configurazione e le relazioni.
- CMDB Visualizer consente di eseguire attività utente e amministrazione per la visualizzazione degli elementi della configurazione e delle relazioni.

Ulteriori informazioni:

Visualizzazione degli elementi della configurazione (a pagina 584)
Creazione di un elemento della configurazione (a pagina 585)
Aggiornamento di un elemento della configurazione (a pagina 585)
Associazione di una finestra di manutenzione con un elemento della configurazione (a pagina 586)
Visualizzazione di finestre di cambiamento associate (a pagina 587)
Visualizzazione della cronologia degli elementi di configurazione (a pagina 587)
Disattivazione di un elemento di configurazione (a pagina 587)
Riattivazione di un elemento di configurazione (a pagina 588)

Visualizzazione degli elementi della configurazione

Il contatore consente di aprire un elemento della configurazione e di visualizzarne le informazioni.

Per aprire e visualizzare un elemento della configurazione, procedere come segue:

1. Dal contatore, selezionare Cerca, Elementi della configurazione.

   Viene visualizzato il riquadro Ricerca elemento della configurazione.

2. Immettere i criteri di ricerca e fare clic su Cerca.

   Viene visualizzato l'Elenco elementi della configurazione contenente i risultati della ricerca.

3. Fare clic su un elemento di configurazione nella colonna Nome per aprirlo e visualizzarne le informazioni dettagliate (facoltativo).

   Vengono visualizzati i dettagli relativi all'elemento della configurazione.

Nota: dopo aver creato un elemento della configurazione, nella pagina Dettagli elemento della configurazione non vengono visualizzati alcuni attributi identificativi perché vuoti (privi di valore) oppure perché se non si applicano alla famiglia dell'elemento della configurazione. Vengono invece visualizzati attributi identificativi con valori non vuoti.

Creazione di un elemento della configurazione

Il Contatore consente di creare un elemento della configurazione.

Per creare un elemento della configurazione

1. Dal contatore, selezionare File, Nuovo elemento della configurazione.

   Viene visualizzata la pagina Crea nuovo elemento della configurazione.

2. Immettere un nome univoco per l'elemento di configurazione nel campo Nome.
3. Immettere la classe dell'elemento di configurazione nel campo corrispondente o fare clic sull'icona della ricerca per individuare una classe.
4. Compilare i campi rimanenti relativi al nuovo elemento di configurazione.

   Nota: solo i valori del campo Nome e Classe sono obbligatori per creare un elemento di configurazione.

5. Fare clic su Continua.

   La pagina Crea nuovo elemento della configurazione visualizza schede e campi aggiuntivi.

6. Immettere i dati nei campi appropriati come richiesto nella scheda Attributi.

   Gli attributi visualizzati sulla scheda vengono determinati dalla famiglia di classi selezionata per l'elemento della configurazione. Le informazioni qui immesse vengono determinate dai processi di business e dalle informazioni che si desidera archiviare e visualizzare per l'elemento della configurazione.

7. Fare clic su Salva.

   Viene visualizzato un messaggio che conferma che l'elemento della configurazione è stato creato.

Aggiornamento di un elemento della configurazione

Il contatore consente di modificare un elemento della configurazione.

Per modificare un elemento della configurazione procedere come segue:

1. Dal contatore, individuare e aprire un elemento della configurazione.

   Viene visualizzata la pagina Dettagli elemento della configurazione.

2. Fare clic su Modifica.

   Viene visualizzata la pagina Aggiorna elemento della configurazione.

3. Apportare le modifiche alle informazioni dell'elemento della configurazione selezionando le schede appropriate nella pagina ed inserendo nuovi dati nei campi. Fare clic su Salva.

   Viene visualizzato un messaggio che conferma che l'elemento della configurazione è stato modificato.

Nota: ogni qual volta un elemento della configurazione viene aggiornato mediante l'opzione –a, la data dell'ultima modifica e l'utente degli elementi della configurazione visualizzati nell'elenco degli elementi della configurazione vengono aggiornati, anche se non è stato modificato alcun attributo. Questo aggiornamento si verifica quando un elemento della configurazione è stato aggiornato nell'interfaccia utente (e salvato senza cambiamenti) o aggiornato mediante GRLoader.

Associazione di una finestra di manutenzione con un elemento della configurazione

Per controllare l'accesso per manutenzione a un elemento della configurazione, è possibile associare tale elemento della configurazione a una o più finestre di manutenzione non globali.

Per associare una finestra di manutenzione con un elemento della configurazione

1. Accedere alla pagina Dettagli elemento della configurazione.
2. Fare clic sulla scheda Finestre manutenzione.

   Viene visualizzato l'Elenco finestre di manutenzione.
3. Fare clic su Aggiorna finestre di manutenzione.

   Viene visualizzata la pagina Ricerca finestre di manutenzione.
4. Specificare le informazioni per le finestre di manutenzione desiderate.
5. Fare clic su Cerca

   Viene visualizzata la pagina delle finestre disponibili.
6. Spostare le finestre desiderate incluse nell'elenco delle finestre di cambiamento disponibili nell'elenco delle finestre di cambiamento associate.
7. Fare clic su OK.

   Vengono salvati l'elemento della configurazione, le finestre di cambiamento e le nuove associazioni delle finestre.

Visualizzazione di finestre di cambiamento associate

Per stabilire come un elemento della configurazione possa essere modificato durante periodi di tempo specifici, è possibile visualizzare le finestre di manutenzione associate a tale elemento della configurazione.

Per visualizzare le finestre di cambiamento associate a un elemento della configurazione

1. Accedere alla pagina Dettagli elemento della configurazione.
2. Fare clic sulla scheda Finestre manutenzione.

   Vengono visualizzate le finestre di manutenzione associate.

Visualizzazione della cronologia degli elementi di configurazione

È possibile visualizzare la cronologia di un elemento della configurazione.

Per visualizzare la cronologia di un elemento della configurazione:

1. Individuare e aprire l'elemento di configurazione.

   Viene visualizzata la pagina Dettagli elemento della configurazione.
2. Fare clic sulla scheda Controllo delle versioni.

   Viene visualizzata la pagina Controllo delle versioni.
3. Fare clic su Mostra registro.

   Viene visualizzata la cronologia dell'elemento di configurazione.

   Nota: l'opzione Mostra registro ignora le selezioni del riquadro sinistro.

Disattivazione di un elemento di configurazione

Se un elemento della configurazione non viene più utilizzato, è possibile modificarne i dettagli per renderlo inattivo. Lo stato inattivo rimuove l'elemento della configurazione dall'elenco di elementi della configurazione nel contatore. Non è possibile eliminare un elemento della configurazione.

Nota: la disattivazione di una famiglia o di una classe non incide sugli elementi della configurazione esistenti inclusi in tale famiglia o classe. Evita solo la creazione di nuovi elementi della configurazione in quella famiglia o in quella classe.

Per disattivare un elemento di configurazione procedere come segue

1. Individuare e aprire l'elemento di configurazione.

   Viene visualizzata la pagina Dettagli elemento della configurazione.

2. Fare clic su Modifica.

   Viene visualizzata la pagina Aggiorna elemento della configurazione.

3. Selezionare Inattivo dall'elenco a discesa Attivo. Fare clic su Salva.

   Viene visualizzato un messaggio di conferma della modifica dello stato. L'elemento di configurazione non viene più visualizzato nell'elenco ci elementi attivi. L'elemento di configurazione continua tuttavia a essere visualizzato in qualsiasi relazione esistente fino a quando tale relazione non viene disattivata.

Riattivazione di un elemento di configurazione

Se è necessario utilizzare un elemento di configurazione inattivo, è possibile riattivarlo.

Per riattivare un elemento di configurazione procedere come segue

1. Individuare e aprire l'elemento di configurazione.

   Viene visualizzata la pagina Dettagli elemento della configurazione.

2. Fare clic su Modifica.

   Viene visualizzata la pagina Aggiorna elemento della configurazione.

3. Selezionare Attivo dall'elenco a discesa Attivo. Fare clic su Salva.

   Viene visualizzato un messaggio di conferma della modifica dello stato. L'elemento di configurazione viene nuovamente visualizzato nell'elenco ci elementi attivi.

Contatto, posizione ed elementi della configurazione dell'organizzazione

Un'installazione CA CMDB è in grado di definire elementi della configurazione per gli *oggetti di base*: contatti, posizioni e organizzazioni. Questi elementi di configurazione possono essere gestiti di conseguenza e possono stabilire relazioni con altri elementi di configurazione, in base alle proprie esigenze. Per alcuni clienti, questo approccio supporta il processo di gestione della configurazione in maniera più efficace rispetto all'impiego esclusivo di oggetti base come gli attributi degli elementi della configurazione.

Ulteriori informazioni:

Creazione di un elemento della configurazione da un oggetto base (a pagina 589)
Selezione di un oggetto di base per un elemento di configurazione (a pagina 590)
Modifica dei dettagli relativi a un elemento della configurazione per un oggetto di base (a pagina 590)
Modifica degli attributi degli elementi della configurazione per un oggetto base (a pagina 591)
Creazione di un elemento di configurazione per un oggetto di base utilizzando GRLoader (a pagina 592)

Creazione di un elemento della configurazione da un oggetto base

Il contatore consente di creare un elemento della configurazione da un oggetto di base.

Per creare un elemento della configurazione da un oggetto di base:

1. Fare clic su File, Nuovo elemento della configurazione.

   Viene visualizzata la pagina Crea nuovo elemento della configurazione.

2. Completare i campi relativi all'elemento della configurazione. Il nome e la classe sono obbligatori. Fare clic su Continua.

   Note: gli attributi comuni per l'elemento di configurazione, nome host, numero di serie, indirizzo MAC e nome DNS non sono rilevanti nel caso di un elemento di configurazione per un oggetto di base.

   Viene visualizzata la pagina Crea nuovo elemento della configurazione.

3. Fare clic sul collegamento dell'oggetto base per definire l'oggetto rappresentato da questo elemento della configurazione.

4. Selezionare l'oggetto. È possibile cercare un oggetto esistente o crearne uno mediante l'opzione Crea nuovo. Se si desidera creare un oggetto, fare clic su Salva per continuare.

   L'oggetto selezionato viene visualizzato in cima alla pagina Dettagli elemento della configurazione.

5. Fare clic su Salva.

   Gli attributi principali dell'oggetto selezionato vengono visualizzati nella scheda Attributi della pagina Dettagli elemento della configurazione dell'oggetto.

Selezione di un oggetto di base per un elemento di configurazione

È possibile selezionare un elemento di base per un elemento di configurazione.

Per selezionare un oggetto di base per un elemento di configurazione procedere come segue

1. Selezionare un elemento di configurazione nella famiglia dell'oggetto di base (Contatto, Ubicazione o Organizzazione).

   Viene visualizzata la pagina Dettagli elemento della configurazione.

2. Fare clic su Modifica.

   Viene visualizzata la pagina Aggiorna elemento della configurazione.

3. Nella sezione superiore, compilare i campi obbligatori relativi all'oggetto di base. È possibile immettere un valore direttamente o fare clic sulla lente di ingrandimento per cercare l'oggetto. Ad esempio, per cercare un contatto, compilare uno o più campi di ricerca nella finestra Ricerca contatto, quindi fare clic su Cerca, poi selezionare il contatto dall'elenco visualizzato.

4. Fare clic su Salva.

   Se l'oggetto selezionato è già rappresentato da un diverso elemento della configurazione nella stessa famiglia, viene visualizzato un messaggio di errore. Selezionare un oggetto differente prima di modificare l'elemento della configurazione.

Modifica dei dettagli relativi a un elemento della configurazione per un oggetto di base

È possibile modificare gli attributi dell'oggetto di base rappresentato dall'elemento della configurazione, quali ID elemento della configurazione alternativo e Note, così come in ogni altra finestra Dettagli elemento della configurazione.

Per modificare gli attributi dell'oggetto di base che l'elemento della configurazione rappresenta

1. Selezionare un elemento della configurazione nella famiglia dell'oggetto di base.

   Viene visualizzata la pagina Dettagli elemento della configurazione.

2. Fare clic sul collegamento dell'oggetto nella parte superiore della pagina.

   Viene visualizzata la pagina Dettagli dell'oggetto.

3. Fare clic su Modifica.

   Viene visualizzata la pagina Aggiorna dell'oggetto.

4. Modificare i campi come desiderato e fare clic su Salva.

   La pagina Aggiorna viene chiusa.

   Se è stato modificato un attributo che viene visualizzato della scheda Attributi della pagina Dettagli elemento della configurazione, il cambiamento viene visualizzato dopo che la pagina viene aggiornata.

Modifica degli attributi degli elementi della configurazione per un oggetto base

È possibile modificare gli attributi relativi a un elemento di configurazione per un oggetto di base.

Per modificare gli attributi relativi a un elemento di configurazione procedere come segue

1. Selezionare un elemento di configurazione nella famiglia dell'oggetto (Contatto, Ubicazione o Organizzazione).

   Viene visualizzata la pagina Dettagli elemento della configurazione.

2. Fare clic su Modifica.

   Viene visualizzata la pagina Aggiorna elemento della configurazione.

3. Sulla scheda Attributi, fare clic su Modifica.

   Viene visualizzata la pagina Aggiorna.

4. Modificare i campi come desiderato e fare clic su Salva.

   La pagina Aggiorna viene chiusa.

5. Fare clic su Salva.

   La pagina Dettagli elemento della configurazione visualizza l'elemento della configurazione modificato.

Creazione di un elemento di configurazione per un oggetto di base utilizzando GRLoader

È possibile utilizzare GRLoader per creare un elemento della configurazione di un oggetto di base da uno esistente.

Per utilizzare GRLoader per creare un elemento della configurazione di un oggetto di base da uno esistente

1. Scrivere un file XML che identifica quanto segue:
   - Nome elemento della configurazione
   - Famiglia
   - Classe
2. Inviare il file XML.

   L'oggetto di base viene creato e GRLoader mostra che un elemento della configurazione è stato letto e inserito.

Esempio: Creazione di un elemento della configurazione da un oggetto esistente

L'esempio seguente illustra la creazione di un elemento di configurazione dal contatto esistente **Gibbs, Keith**.

```
<GRLoader>
<ci>
    <name>Gibbs, Keith</name>
    <family>Contatto</family>
    <class>Tecnico</class>
    <base_contact>Gibbs, Keith</base_contact>
<ci>
</GRLoader>
```

Relazioni elemento della configurazione

La funzionalità di CA SDM dipende dalle relazioni tra gli elementi della configurazione. Le relazioni degli elementi della configurazione hanno le caratteristiche seguenti:

- Il *tipo di relazione* definisce la correlazione tra gli elementi della configurazione.
- Le relazioni di tipo gerarchico sono correlate come *fornitore/dipendente*. Ad esempio, A (fornitore) *ospita* B; B (dipendente) *è ospitato da* A.
- Le relazioni di tipo non gerarchico sono definite come *peer to peer*. Ad esempio, *è connesso a*, che è valida in entrambe le direzioni.

È possibile eseguire le seguenti funzioni di relazione utilizzando la scheda Relazioni CMDB:

- Visualizzare relazioni attive o non attive eseguendo una ricerca sul campo Attivo? campo.
- Nell'Elenco relazioni elementi della configurazione, è possibile fare clic su qualsiasi collegamento di una relazione per visualizzarne la pagina Dettagli relazione elemento della configurazione.

Ulteriori informazioni:

Tipi relazioni elementi della conoscenza (a pagina 593)
Creazione di un tipo di relazione (a pagina 594)
Gestione della relazione degli elementi della configurazione (a pagina 595)
Creazione di una relazione degli elementi della configurazione (a pagina 595)
Visualizzazione delle relazioni per un elemento di configurazione (a pagina 596)
Disattivazione di una relazione di un elemento della configurazione (a pagina 596)
Riattivazione di una relazione degli elementi della configurazione (a pagina 597)
Disattivazione di relazioni di elementi della configurazione (Modifica in elenco) (a pagina 597)
Disattivazione di una relazione dell'elemento della configurazione utilizzando GRLoader (a pagina 598)
Riattivazione di una relazione dell'elemento della configurazione utilizzando GRLoader (a pagina 599)
Eliminazione di una relazione di elementi della configurazione dal database (a pagina 600)
Cronologia e confronto di una relazione di elemento della configurazione (a pagina 600)

Tipi relazioni elementi della conoscenza

CA SDM fornisce un elenco di tipi di relazione predefiniti che è possibile utilizzare per descrivere una relazione o associazione tra elementi della configurazione. Il modo in cui viene espressa una relazione dipende dall'elemento della configurazione attivo. Ad esempio, un fornitore *supporta* un elemento della configurazione dipendente, ma il dipendente *è supportato dal* fornitore. Queste sono espressioni differenti della stessa relazione e l'etichetta del tipo di relazione visualizzata all'utente varia a seconda che si stia visualizzando una relazione da fornitore a dipendente o da dipendente a fornitore.

Nota: per ulteriori informazioni sui tipi di relazione offerti da CA CMDB, vedere la *Guida di riferimento tecnico CA CMDB*.

Creazione di un tipo di relazione

È possibile creare un tipo di relazione e renderla disponibile per creare o aggiornare relazioni.

Per creare un tipo di relazione

1. Nella scheda Amministrazione, espandere la cartella CA CMDB visualizzata nel riquadro sinistro.
2. Fare clic su Tipi di relazione tra elementi della configurazione.

   Nel riquadro di destra viene visualizzato l'Elenco tipo relazione elemento della configurazione.
3. Fare clic su Crea nuovo.

   Viene visualizzata la pagina per la creazione di un nuovo tipo di relazione tra elementi della configurazione.
4. Inserire i dati nei seguenti campi:

   Etichetta Da fornitore a dipendente

   Descrive la relazione da fornitore a dipendente ed è il nome che compare nell'elenco dei tipi di relazione. Ad esempio, "servizi" o "gestisce" è una relazione da fornitore a dipendente.

   Etichetta Da dipendente a fornitore

   Descrive la relazione da dipendente a fornitore ed è il nome che compare nell'elenco dei tipi di relazione. Ad esempio, "è fornito da" o "è gestito da" è una relazione da dipendente a fornitore.

   Peer-to-Peer?

   Specifica che la relazione non ha un elemento della configurazione fornitore e uno dipendente, ma consiste in due elementi della configurazione di pari livello. Ad esempio, "si connette a" ed "esegue il failover" sono relazioni peer to peer.

   Attivare?

   Rende il tipo di relazione selezionabile in relazioni di elementi della configurazione e visualizzabile negli elenchi.
5. Fare clic su Salva.

   Il tipo di relazione viene creato e sarà disponibile per creare o aggiornare le relazioni.

Gestione della relazione degli elementi della configurazione

La pagina Relazione elemento della configurazione fornisce tutte le impostazioni necessarie in un'unica posizione per semplificare il processo di relazione degli elementi della configurazione.

È possibile utilizzare la pagina per eseguire le seguenti funzioni:

- Commutare la relazione fornitore/dipendente tra due elementi della configurazione.

  Fare clic su Inverti per invertire l'elemento della configurazione fornitore e l'elemento della configurazione dipendente per la relazione. L'elemento della configurazione con stato attivo cambia. Se la relazione invertita non è valida, facendo clic su Inverso il campo Relazione viene annullato.

- Impostare i campi opzionali come Simbolo, Descrizione e Costo.

  Fare clic cu Facoltativo per impostare campi facoltativi.

  Se non viene fornito un simbolo, quando si crea la relazione viene automaticamente generato un simbolo univoco con il prefisso **cmdb bmhier:** e un numero univoco.

  Nota: se l'installazione è integrata con CA Network and Systems Management (CA NSM), viene richiesto di specificare il repository CA NSM e il costo.

Creazione di una relazione degli elementi della configurazione

È possibile aggiungere una relazione degli elementi della configurazione a partire da un elemento della configurazione attivo.

Per aggiungere una relazione partendo da un elemento della configurazione attivo

1. Selezionare l'elemento di configurazione a cui si desidera aggiungere una relazione.

   Viene visualizzata la pagina dei dettagli dell'elemento della configurazione.

2. Fare clic su Modifica.

   Viene visualizzata la pagina Aggiorna elementi della configurazione.

3. Fare clic sulla scheda Relazioni CMDB, quindi su Crea nuovo.

   Viene visualizzata la pagina per la creazione di una nuova relazione tra elementi della configurazione.

4. Specificare l'elemento di configurazione fornitore. È possibile fare clic sul collegamento della lente di ingrandimento per cercare l'elemento della configurazione.

   Nota: a seconda del tipo di relazione desiderata, è possibile fare clic su Inverti per passare dalla posizione di fornitore a quella di dipendente e viceversa.

5. Specificare un tipo di relazione. È possibile fare clic sul collegamento della lente di ingrandimento per cercare il tipo di relazione.

6. Specificare l'altro elemento della configurazione (per impostazione predefinita, quello dipendente). È possibile fare clic sulla lente di ingrandimento per ricercare l'elemento di configurazione.

7. Fare clic su Salva.

   La relazione verrà creata.

Visualizzazione delle relazioni per un elemento di configurazione

È possibile visualizzare le relazioni per un elemento della configurazione.

Per visualizzare le relazioni per un elemento della configurazione

1. Accedere all'elemento della configurazione.

   Viene visualizzata la pagina Dettagli elemento della configurazione.

2. Selezionare la scheda Relazioni CMDB.

   Viene visualizzato un elenco di relazioni per l'elemento della configurazione.

Disattivazione di una relazione di un elemento della configurazione

È possibile disattivare una relazione di un elemento della configurazione impostandone lo stato su Non attivo.

Per disattivare una relazione

1. Accedere alla pagina relativa ai dettagli degli elementi della configurazione, fare clic sulla scheda Relazioni CMDB, quindi su Modifica.

   La scheda Relazioni CMDB viene visualizzata in modalità Modifica.

2. Scegliere una relazione e fare clic su un collegamento qualsiasi sulla relativa riga.

   Viene visualizzata la pagina Dettagli relazione elemento della configurazione.

3. Fare clic su Modifica.

4. Impostare l'attributo Active? su Inattivo. Fare clic su Salva.

   La relazione diventa inattiva. Nella pagina Dettagli relazione elemento della configurazione, l'attributo “Attivo?” visualizza il valore di attributo Non attivo.

Riattivazione di una relazione degli elementi della configurazione

È possibile riattivare una relazione degli elementi della configurazione eliminata.

Per riattivare una relazione degli elementi della configurazione eliminata

1. Accedere alla pagina Dettagli elemento della configurazione.

   Viene visualizzata la pagina Dettagli elementi della configurazione in modalità di sola lettura.

2. Fare clic su Modifica.

   Viene visualizzata la pagina Dettagli elementi della configurazione in modalità di modifica.

3. Fare clic sulla scheda Relazioni CMDB.
4. Fare clic su qualsiasi collegamento visualizzato in una riga per aprire la pagina Dettagli relazione elemento della configurazione.
5. Fare clic su Modifica.

   Viene visualizzata la pagina Aggiorna relazione elemento della configurazione.

6. Modificare l'attributo Active? su "Attivo". Fare clic su Salva.

   La relazione viene riattivata.

Disattivazione di relazioni di elementi della configurazione (Modifica in elenco)

È possibile disattivare una o più relazioni degli elementi della configurazione utilizzando la funzionalità Modifica in elenco.

Per disattivare una o più relazioni degli elementi della configurazione

1. Dalla scheda Amministrazione, aprire la cartella CA CMDB visualizzata nel riquadro sinistro.

   Il nodo CA CMDB si espande in modo da visualizzare le sottocartelle.

2. Fare clic sulla cartella Elenco relazioni elementi della configurazione.
3. (Facoltativo) Specificare i filtri di ricerca
4. Fare clic su Cerca.

   Le relazioni degli elementi della configurazione sono visualizzate nel riquadro destro.

   Nota: per impostazione predefinita, vengono visualizzate tutte le relazioni.

5. Fare clic su Modifica in elenco, nella parte superiore destra dell'elenco.

   Vengono visualizzati i controlli Modifica in elenco della relazione.

6. Selezionare la riga contenente la relazione che si desidera modificare.

   Viene visualizzata la riga e i controlli vengono riempiti con i valori della relazione.

7. Impostare l'attributo Active? su Inattivo.

   Fare clic su Salva per disattivare solo la relazione evidenziata o su Modifica tutto per disattivare tutte le relazioni nella ricerca filtrata.

Disattivazione di una relazione dell'elemento della configurazione utilizzando GRLoader

È possibile disattivare una relazione di un elemento della configurazione utilizzando GRLoader per inviare il file XML.

Per disattivare una relazione utilizzando GRLoader

1. Scrivere un file XML che utilizzi un tag di relazione per identificare quanto segue:
   - Elemento della configurazione provider
   - Elemento della configurazione dipendente
   - Tipo di relazione
2. Impostare delete_flag su true (oppure yes o 1).
3. Inviare il file XML.

   La relazione degli elementi della configurazione viene eliminata.

Nota: per ulteriori informazioni su GRLoader, vedere la *Guida di riferimento tecnico CA CMDB*.

Esempio: Eliminazione di una relazione degli elementi della configurazione tramite GRLoader

Nel seguente esempio relativo a XML, la relazione "si connette a" tra ci_1 e ci_2 viene eliminata.

```
<GRLoader>
        <relation>
                <dependent>
                        <name>ci_2</name>
                </dependent>
        <type>si connette a</type>
                <provider>
                        <name>ci_1</name>
                </provider>
        <delete_flag>true</delete_flag>
        </relation>
</GRLoader>
```

Riattivazione di una relazione dell'elemento della configurazione utilizzando GRLoader

È possibile riattivare una relazione degli elementi della configurazione utilizzando GRLoader per inviare l'XML.

Riattivazione di una relazione di un elemento della configurazione utilizzando GRLoader

1. Scrivere un file XML che utilizzi un tag di relazione per identificare quanto segue:
   - Tipo di relazione
   - Elemento della configurazione dipendente
   - Elemento della configurazione provider
2. Impostare delete_flag su false (oppure no o 0).
3. Inviare il file XML.

   La relazione degli elementi della configurazione viene riattivata.

Nota: per ulteriori informazioni su GRLoader, vedere la *Guida di riferimento tecnico CA CMDB*.

Esempio: Riattivazione di una relazione degli elementi della configurazione

Nel seguente esempio relativo a XML, la relazione "si connette a" tra ci_1 e ci_2 viene riattivata.

```
<GRLoader>
        <relation>
                <dependent>
                        <name>ci_2</name>
                </dependent>
        <type>si connette a</type>
                <provider>
                        <name>ci_1</name>
                </provider>
        <delete_flag>false</delete_flag>
        </relation>
</GRLoader>
```

Eliminazione di una relazione di elementi della configurazione dal database

È possibile eliminare una relazione di un elemento della configurazione in modo che non venga semplicemente disattivata ma rimossa in modo permanente dal database.

Per rimuovere una relazione dal database

1. Accedere all'Elenco relazioni elemento della configurazione.

   Viene visualizzato l'Elenco relazioni elemento della configurazione.

2. Fare clic con il pulsante destro del mouse su qualsiasi riga di relazione e selezionare Elimina.

   La relazione viene rimossa dal database.

Importante: se per la relazione eliminata è stato definito un simbolo, eventuali altre relazioni con lo stesso simbolo vengono anch'esse rimosse dal database.

Cronologia e confronto di una relazione di elemento della configurazione

La scheda Controllo delle versioni mostra le relazioni degli elementi della configurazione e consente di eseguire le seguenti operazioni:

- Visualizzare la cronologia delle relazioni per qualsiasi elemento della configurazione in CMDB. Le modifiche apportate a una relazione sono registrate automaticamente al momento della creazione, dell'aggiornamento o dell'eliminazione della relazione stessa. È possibile visualizzare tutte le relazioni correnti e passate per un elemento della configurazione.

  Nota: le relazioni create con le versioni precedenti di CA CMDB non dispongono delle informazioni relative alla cronologia di audit.

- Confrontare le relazioni in qualsiasi snapshot o attività cardine.

Controllo delle versioni

Il controllo delle versioni promuove il controllo dell'infrastruttura IT tracciando e gestendo i cicli di vita di tutti gli elementi della configurazione che costituiscono lo stato autorizzato del CMDB. Il controllo delle versioni si applica anche alla verifica della cronologia di un oggetto. Il controllo delle versioni fornisce le seguenti funzioni per il controllo dell'infrastruttura IT:

Snapshot

Registrato automaticamente per i cambiamenti apportati al valore di qualsiasi aggiornamento a un oggetto, ad esempio quando si aggiorna un elemento della configurazione. Il controllo delle versioni crea una snapshot che registra lo stato completo dell'elemento della configurazione hardware in seguito alla modifica delle dimensioni della memoria di un computer. Il controllo delle versioni può visualizzare la snapshot e indicare quali attributi dell'elemento della configurazione sono cambiati. Inoltre, è possibile eseguire un confronto con tutte le snapshot della cronologia dell'elemento della configurazione. Questa informazione di estrema importanza è indispensabile quando si cerca di comprendere l'impatto dei cambiamenti sulla disponibilità e sulle prestazioni di un elemento della configurazione.

Cardini

I cardini vengono registrati come istantanee speciali con etichetta definita dall'utente, ad esempio Primo giorno di produzione o Baseline di gennaio. Queste etichette consentono di individuare snapshot specifiche più rapidamente.

Importante. I cardini *non* vengono applicati a specifiche del Cambiamento, policy di verifica, stati del Cambiamento gestiti e attributi gestiti.

Confronti

È possibile eseguire il confronto di un elemento della configurazione con un altro che funge da elemento standard. Sebbene sia possibile utilizzare qualsiasi elemento della configurazione come standard per il confronto, si consiglia di utilizzare elementi specifici quali gli *elementi della configurazione standard*. Un elemento della configurazione standard consente di definire una configurazione standard rispetto alla quale confrontare altri elementi della configurazione operativi appartenenti alla stessa famiglia. Ad esempio, un'organizzazione può decidere di definire Server di grandi dimensioni come un elemento standard della configurazione standard per fissare i valori attributo che definiscono questo tipo di server. L'elemento della configurazione standard per una famiglia può diventare l'attributo di un elemento della configurazione operativo di tale famiglia, che consente di confrontare lo stato attuale o qualsiasi stato storico di un elemento della configurazione con la relativa configurazione standard associata. Analogamente agli altri confronti, queste informazioni possono essere stampate o esportate in un file con valori separati da virgola.

Mentre i milestone possono fungere da linee di base non condivise né modificabili, gli elementi di configurazione standard forniscono linee di base dinamiche e condivise per i propri elementi di configurazione.

Importante. Un elemento della configurazione standard non deve mai contenere valori per attributi utilizzati per la riconciliazione degli elementi della configurazione.

Specifiche del Cambiamento

È possibile visualizzare le specifiche del Cambiamento pianificate o non pianificate indicate da un utente per gli Ordini di cambiamento dell'elemento della configurazione. È possibile confrontare la specifica del cambiamento con lo stato attuale dell'elemento della configurazione. Ad esempio, confrontare un valore pianificato con lo stato attuale di un elemento della configurazione. Questo confronto può mostrare eventuali conflitti con i cambiamenti, identificare i cambiamenti che si sovrappongono nella pianificazione, ecc.

Il controllo delle versioni consente di completare le attività seguenti:

- Acquisizione automatica di tutte le modifiche agli elementi della configurazione
- Snapshot di un elemento della configurazione in corrispondenza di un punto temporale qualsiasi sulla base delle modifiche di date o attributi
- Diversi livelli di visualizzazione, tra cui il registro dettagliato e le visualizzazioni di base e avanzate.

- Confronti di più attributi con altre snapshot, con milestone definiti dagli utenti per gli elementi della configurazione o con un elemento della configurazione standard
- Snapshot automatiche ogni volta che CA SDM modifica lo stato dei ticket

  Nota: questa snapshot automatica non è valida per specifiche del Cambiamento, policy di verifica, stati del Cambiamento gestito e attributi gestiti.
- Funzionalità di filtro e confronto avanzate con supporto di stampa ed esportazione in formato .csv

Ulteriori informazioni:

Utilizzo del controllo delle versioni (a pagina 603)
Record di audit trail per asset ed elementi della configurazione condivisi (a pagina 604)
Terminologia relativa al controllo delle versioni (a pagina 605)
Origini dei dati di controllo delle versioni (a pagina 608)
Integrazione della gestione della modifica SDM degli elementi della configurazione (a pagina 609)
CA APM Integrazione (a pagina 610)
Gestione del controllo delle versioni degli elementi della configurazione (a pagina 611)
Gestione delle modifiche in CA SDM (a pagina 632)
Funzionalità CACF (Configuration Audit and Control Facility) (a pagina 703)
Controllo delle versioni e stato futuro dell'elemento della configurazione (a pagina 729)

Utilizzo del controllo delle versioni

Il controllo delle versioni comprende quanto segue:

Identificazione di un problema

Per correggere un problema con un elemento della configurazione *è necessario* verificare le modifiche apportate all'ambiente dell'elemento della configurazione. Il controllo delle versioni mostra lo stato di errore corrente e precedente, consentendo di confrontare due stati per individuare i potenziali problemi.

Pianificazione delle prestazioni e della capacità

Rivedendo la cronologia di un elemento della configurazione, un pianificatore di prestazioni o di capacità ha maggiore possibilità di determinare le cause dei problemi e di eseguire pianificazioni per l'espansione futura del sistema.

Conformità

È possibile confrontare lo stato di un elemento della configurazione con lo stato di un elemento della configurazione standard della stessa famiglia. Il confronto dello stato in un punto qualsiasi del ciclo di vita della gestione del Cambiamento, consente di verificare la conformità dell'elemento della configurazione e individuare gli attributi che richiedono la correzione.

Verifica del Cambiamento

È possibile visualizzare la cronologia di audit dell'oggetto, ad esempio l'utente che ha modificato una policy di verifica, la data della Richiesta, gli attributi e i valori modificati dall'utente. È possibile confrontare e contrastare le modifiche apportate tra date specifiche.

Record di audit trail per asset ed elementi della configurazione condivisi

La funzionalità di controllo delle versioni include i cambiamenti di audit trail apportati a CA APM. La funzionalità di controllo delle versioni supporta anche l'avvio diretto nel contesto da CA CMDB a CA APM da una voce di registro attributo associata a una modifica CA APM. Le informazioni di audit trail di CA APM sono disponibili solo per gli elementi della configurazione/asset provenienti da famiglie CA CMDB con la registrazione di audit CA APM attivata.

La scheda Controllo delle versioni che include le informazioni sull'itinerario di controllo di CA APM supporta tutte le famiglie, a condizione che la registrazione per la famiglia in questione sia abilitata.

Per impostazione predefinita, CA APM non registra i cambiamenti di attributo dell'asset. Per utilizzare il controllo delle versioni di CA CMDB con un elemento della configurazione/asset gestito da CA APM, è necessario attivare l'opzione Archivia dati audit trail per ciascun attributo di asset da registrare.

Nota: per ulteriori informazioni sulla modalità di attivazione dell'audit, consultare la documentazione di CA APM.

Quando in CA APM vengono modificati gli attributi dell'asset, i dati della scheda relativa al controllo delle versioni nella pagina Dettagli elemento della configurazione potrebbero essere aggiornati prima dei dati della scheda Attributi; ciò è dovuto all'impiego della cache. Per risincronizzare i valori, fare clic sul pulsante Modifica.

Terminologia relativa al controllo delle versioni

Il controllo delle versioni è la procedura utilizzata per registrare e tenere traccia delle *transizioni del servizio*. In genere, questo processo utilizza una convenzione di denominazione per identificare le date, le sequenze e i significati di tali transizioni. Le registrazioni di questi elementi possono essere utilizzate per identificare e confrontare gli stati specifici di un elemento di configurazione.

Esempio: Confronto di versione

Per l'elemento di configurazione di un'applicazione di gestione delle buste paga, un confronto tra la versione 3 e la versione 2 mostra le funzionalità avanzate e altre differenze della versione più recente.

Ulteriori informazioni:

Stati (a pagina 605)
Versioni (a pagina 605)
Snapshot (a pagina 605)
Categorie (a pagina 606)
Cardini (a pagina 606)
Elementi della configurazione standard (a pagina 607)

Stati

Nel contesto di Controllo versione, lo *stato* di un elemento di configurazione rappresenta tutti i valori degli attributi di tale elemento in un singolo momento. Lo stato di un elemento di configurazione può essere il risultato delle modifiche degli attributi derivanti da più MDR.

Versioni

Una *versione* corrisponde a un'istanza identificata di un oggetto, ad esempio un elemento della configurazione, entro la suddivisione o la struttura di configurazione di un prodotto. Le versioni vengono utilizzate per tenere traccia ed eseguire l'audit della cronologia del Cambiamento.

Snapshot

Una *snapshot* è una rappresentazione dello stato completo di un oggetto in un determinato momento. Generalmente, a un elemento della configurazione sono associate più snapshot. Una snapshot consolida tutte le modifiche apportate a un oggetto durante un intervallo di un minuto. Ad esempio, se un elemento di configurazione viene aggiornato (modificato e salvato) più volte in un minuto, CA SDM crea una sola snapshot contenente tutti gli aggiornamenti eseguiti durante tale intervallo di tempo.

Snapshot è un termine generico che fa riferimento alle snapshot basate su data e ora, nonché ai cardini o agli elementi della configurazione standard. Per individuare più facilmente i momenti significativi, CA SDM consente di aggiungere un'etichetta alle snapshot. Tali snapshot sono denominate cardini.

Ogni volta che viene apportata una modifica a un elemento della configurazione, CA SDM crea automaticamente una snapshot, senza la necessità di intervento manuale da parte dell'utente. Il controllo delle versioni include tutte le modifiche apportate all'oggetto. Ad esempio, le snapshot create mediante l'interfaccia utente oppure le snapshot generate in un MDR e trasferite a CMDB attraverso GRLoader o i servizi Web di CA CMDB.

Categorie

Una *categoria* identifica una classe di attributi. Generalmente la categoria corrisponde al nome della scheda in cui sono visualizzati gli attributi.

Nota: agli elementi non inclusi in una scheda, ad esempio nome, numero di serie e flag attivo viene assegnata una categoria che non è un nome di scheda.

Esempi: schede e categorie

I seguenti esempi mostrano il modo in cui le categorie corrispondono alle schede:

- Poiché lo *spazio su disco* viene visualizzato nella scheda Attributi, la relativa categoria è *Attributi*.
- Poiché l'*indirizzo IP* viene visualizzato nella scheda Inventario, la relativa categoria è *Inventario*.
- I*cardini* vengono visualizzati nella categoria *Generale*.
- Un *elemento di configurazione standard* viene visualizzato nella categoria Classificazione.
- Le *relazioni* vengono visualizzate nella categoria Relazione.

Cardini

Un *cardine* corrisponde alla snapshot di un elemento della configurazione con etichetta on-demand che viene creata per contrassegnare un evento, un breakpoint logico o un accumulo di modifiche. Il cardine contiene lo stato effettivo dell'elemento della configurazione al momento della creazione della snapshot. I cardini consentono di identificare e accedere velocemente ai punti significativi della cronologia di un elemento della configurazione. La creazione di un cardine comporta la creazione di una snapshot di "data" equivalente.

Ciascun cardine è specifico di un elemento della configurazione, pertanto non sono condivisi. Quando si crea un cardine per un oggetto di livello elevato, ad esempio un servizio, i componenti secondari di tale oggetto di livello elevato non eseguono la creazione automatica del cardine. Per utilizzare un cardine composto da più componenti secondari, è possibile creare più cardini indipendenti.

I cardini sono statici e non possono essere modificati o eliminati. Quando si crea un cardine, la snapshot presenta lo stesso stato dell'elemento della configurazione. Inoltre, se visualizzati o utilizzati in un confronto, fanno sempre riferimento a un punto specifico nel passato. Una convenzione di denominazione efficace dei cardini consente di identificare più facilmente i punti critici nella vita di un elemento della configurazione.

Importante. I cardini *non* vengono applicati a specifiche del Cambiamento, policy di verifica, stati del Cambiamento gestiti e attributi gestiti.

Elementi della configurazione standard

Un *elemento della configurazione standard* è una configurazione separata per una famiglia di elementi della configurazione utilizzabile per i confronti di linea di base con le istanze "reali" dell'elemento della configurazione nella stessa famiglia. Un elemento della configurazione standard può essere un vero elemento della configurazione, nel senso che rappresenta un oggetto fisico, o può avere solo scopi di comparazione. Gli elementi della configurazione standard possono avere le seguenti associazioni:

- Un elemento della configurazione standard può essere condiviso da più elementi della configurazione.
- In un determinato momento, a un elemento della configurazione può essere associato uno solo elemento della configurazione standard. Quando l'elemento della configurazione standard viene modificato, tale modifica viene riflessa in ogni confronto tra questo e gli elementi della configurazione associati.
- Una famiglia può includere più elementi di configurazione standard. Ad esempio, una famiglia può includere elementi di configurazione standard denominati "Server di test standard", "Server di produzione standard" e "Server di accettazione standard". Si consiglia di denominare gli elementi di configurazione standard in modo tale da rendere possibile ricercarli e identificarli come elementi di configurazione di tale tipo.

Poiché un elemento di configurazione standard è di per sé un elemento di configurazione, può essere gestito. È dotato delle funzionalità di audit trail, protezione, cronologia delle modifiche, ecc., come qualsiasi altro elemento della configurazione. Una volta definito un elemento della configurazione standard per un elemento della configurazione specifico, è possibile utilizzarlo per verificare la conformità con gli standard aziendali.

Il concetto di "data" o "ora" non è applicabile quando si esegue il confronto tra un elemento della configurazione standard e una snapshot o un'attività cardine. Solo i valori degli attributi dell'elemento della configurazione standard vengono utilizzati a scopo di confronto; le snapshot e le attività cardine specifiche dell'elemento della configurazione standard non vengono considerate.

Esempio: Utilizzo dell'elemento della configurazione standard

Un'azienda definisce una configurazione **workstation del dipendente** come elemento della configurazione standard da confrontare con i computer desktop effettivi nella famiglia di Hardware.Workstation. Un confronto mostra che un computer specifico è dotato di 1 solo GB di RAM, anziché della quantità di memoria di 2 GB dell'elemento della configurazione standard.

Origini dei dati di controllo delle versioni

I dati di controllo delle versioni vengono generati dai componente in grado di supportare la funzionalità del registro di audit in seguito alla creazione o modifica di un oggetto. Non è possibile distinguere le snapshot generate da più origini. Quando l'ambiente è configurato correttamente, le snapshot vengono visualizzate in modo automatico ogni volta che vengono apportate modifiche agli elementi di configurazione e alle relative relazioni.

Tutte le famiglie di CA CMDB sono attivate per il controllo versioni. Tuttavia, per poter utilizzare questa funzione, gli elementi della configurazione contenuti nelle famiglie di CA Service Desk devono essere convertiti in famiglie di CA CMDB.

Il controllo delle versioni include le seguenti fonti:

- **Aggiornamenti dell'elemento della configurazione CA CMDB** — Consente di eseguire l'aggiornamento degli attributi degli elementi della configurazione comuni e degli attributi degli elementi della configurazione specifici della famiglia utilizzando l'interfaccia utente.
- **Aggiornamenti delle relazioni di CA CMDB** — Consente di aggiornare le relazioni nella scheda Relazioni CMDB e nell'Elenco relazioni elementi della configurazione mediante la funzionalità Modifica e Modifica in elenco.

- **GRLoader** — Aggiornamento degli inserimenti e degli attributi degli elementi della configurazione, aggiornamento delle relazioni, assegnazioni degli elementi della configurazione standard e cardini importati mediante GRLoader. Quando gli aggiornamenti da un MDR vengono inviati utilizzando GRLoader, viene anche registrata l'origine MDR. Questo consente di tenere traccia delle modifiche apportate agli attributi direttamente all'origine.

  Nota: per ulteriori informazioni, consultare la *Guida di riferimento tecnico*.

- **Cronologia dei Cambiamenti CA SDM** — Viene creata automaticamente una snapshot per tutti gli elementi della configurazione associati a un ticket di Cambiamento. Vengono create fino a quattro snapshot corrispondenti a quando l'elemento di configurazione viene aperto, chiuso, attivato o risolto.
- **Modifiche agli elementi della configurazione di CA Asset Portfolio Management (CA APM)** — Cambiamenti effettuate da CA APM agli elementi della configurazione con registrazione attivata.
- **Verifica del Cambiamento** — Aggiornamento delle specifiche del Cambiamento, delle policy di verifica, degli stati del Cambiamento gestito e degli attributi gestiti.

Nota: gli elementi della configurazione creati in CA SDM o nelle versioni precedenti di CA CMDB contengono unicamente le modifiche dei Cambiamenti. I valori iniziali degli attributi, ad esempio nome, famiglia e classe non vengono registrati e non sono visualizzati nelle snapshot. Inoltre, le relazioni create con CA Service Desk o con versioni di CA CMDB precedenti non includono informazioni sulla cronologia di audit.

Integrazione della gestione della modifica SDM degli elementi della configurazione

I dati di controllo delle versioni vengono generati per ciascun elemento della configurazione associato al ticket delle modifiche di CA SDM. Mentre il ticket delle modifiche passa da aperto ad attivo, quindi a risolto e a chiuso, viene creata una snapshot per ciascuno degli elementi della configurazione associati. Pertanto le snapshot vengono create per gli stati aperto, chiuso, attivo o risolto. Se a una richiesta di modifica non sono associati elementi della configurazione, non viene creata alcuna snapshot.

Nota: questa funzione non richiede operazioni di configurazione speciali ed è supportata in modo automatico nelle installazioni integrate.

La funzione di controllo versioni gestisce il ticket delle modifiche come segue:

1. Confronta la stato dell'elemento della configurazione al momento dell'apertura con lo stato corrente.
2. Verifica che tutte le modifiche richieste siano state eseguite correttamente e che non siano state aggiunte ulteriori modifiche.
3. Chiude il ticket dopo la validazione delle modifiche.

È possibile confrontare immediatamente lo stato dell'elemento della configurazione prima e dopo ciascuna modifica, a scopo di audit. Queste informazioni di confronto aiutano nella risposta delle domande, come quelle relative allo stato di un elemento della configurazione, prima e dopo una richiesta di modifica. Ad esempio:

- La modifica appropriata è stata eseguita come richiesto?
- Quali altre modifiche sono state eseguite nell'elemento della configurazione non in relazione al ticket delle modifiche?
- A che ora sono state eseguite le modifiche?
- Quali risultati restituisce il confronto dell'elemento di configurazione con la configurazione standard prima e dopo la modifica?

CA APM Integrazione

Il controllo delle versioni visualizza le modifiche eseguita da CA APM ai propri elementi della configurazione. Il controllo delle versioni supporta inoltre l'avvio diretto nel contesto da CA CMDB a CA APM da una voce di registro attributo associata a una modifica CA APM. Le informazioni di audit CA APM sono disponibili solo per gli elementi della configurazione provenienti da famiglie CA CMDB quando la registrazione di audit CA APM è attivata.

Nota: quando in CA APM vengono modificati gli attributi degli elementi della configurazione, i dati della scheda Controllo delle versioni nella pagina relativa ai dettagli dell'elemento della configurazione potrebbero essere aggiornati prima di quelli della scheda Attributi; ciò è dovuto all'impiego della cache. Per risincronizzare i valori, fare clic sul pulsante Modifica.

Per impostazione predefinita, CA APM non registra le modifiche degli attributi degli elementi della configurazione. Per utilizzare il controllo delle versioni con un elemento della configurazione gestito da CA APM è necessario attivare l'opzione Archivia dati audit trail per ciascun attributo di asset da registrare.

Per impostazione predefinita, si verifica un ritardo di dieci minuti tra il momento in cui un elemento della configurazione viene aggiornato in CA APM e il momento in cui diviene disponibile per il controllo versioni in CMDB. È possibile ottenere un ritardo diverso modificando la variabile @NX_DBMONITOR_TIMER_MINUTES in un'installazione integrata.

Nota: per informazioni su come attivare la registrazione degli attributi per gli asset, consultare la documentazione di CA APM.

Ulteriori informazioni:

Capacità di integrazione di CA APM (a pagina 611)

Capacità di integrazione di CA APM

CA SDM fornisce le seguenti funzionalità di integrazione con CA APM:

- Record condivisi e registro di audit che distinguono tra elementi della configurazione e asset CA APM
- Avvio nel contesto CA CMDB e CA APM degli elementi della configurazione/asset
- Campi condivisi delle tabelle estensioni
- Un contatto CA SDM viene aggiornato quando CA APM modifica un contatto primario
- Modifica del tipo di asset CA APM per l'utilizzo delle famiglie degli elementi della configurazione

Gestione del controllo delle versioni degli elementi della configurazione

È possibile visualizzare e gestire la cronologia dell'elemento della configurazione, le snapshot associate, i cardini, i cambiamenti non pianificati e altre visualizzazioni. Il riquadro sinistro consente di navigare, mentre in quello destro è possibile visualizzare i dettagli dell'elemento della configurazione e il registro di audit.

Nota: il controllo delle versioni funziona allo stesso modo per la cronologia dell'attributo gestito e per la cronologia stato del Cambiamento gestito. Ad esempio, la scheda Cronologia attributo gestito visualizza informazioni di controllo delle versioni relative a un attributo gestito.

Utilizzare le informazioni del controllo delle versioni per individuare le specifiche del Cambiamento e gli Ordini di cambiamento associati. Il controllo delle versioni identifica i cambiamenti non pianificati nelle specifiche del cambiamento nella visualizzazione della snapshot che corrispondono agli ordini di cambiamenti senza una data di avvio pianificata. È possibile visualizzare la snapshot e il registro di una specifica del cambiamento in CACF.

Esempio: Cambiamento non pianificato

In questo esempio, un utente desidera modificare il valore di un attributo gestito. Si visualizza la scheda Controllo delle versioni nella pagina dei dettagli dell'elemento della configurazione che visualizza i cambiamenti non pianificati nella snapshot. Questa snapshot visualizza informazioni sul cambiamento, ad esempio la data, l'ora, il nome utente e il valore attributo.

Quando si seleziona una snapshot o un'attività cardine nel riquadro sinistro, nel riquadro destro vengono visualizzati i valori degli attributi dello stato, dell'evento o del confronto dell'elemento della configurazione. Il riquadro sinistro può visualizzare le snapshot degli elementi della configurazione o i cardini in base alla data e ora (modalità Base) o in base alle caratteristiche degli elementi della configurazione (modalità Avanzata), e comprende i collegamenti seguenti per la gestione di un elemento della configurazione:

Crea cardine

Etichetta lo stato di un elemento della configurazione.

Mostra registro

Visualizza la cronologia non filtrata dell'elemento della configurazione.

Avanzata/Di base

Consente di passare da una visualizzazione snapshot all'altra.

Nascondi valori vuoti

Consente il filtraggio di campi dati vuoti. Non non si seleziona questa opzione, vengono visualizzati tutti gli attributi degli elementi della configurazione.

Stampa ed Esporta

Consentono di eseguire operazioni di stampa o taglia e incolla per salvare i dati del controllo versione.

Mostra registro

Il registro consente di visualizzare una cronologia dell'elemento della configurazione. L'opzione Filtro consente di filtrare le righe del registro. Stampa ed Esporta consentono di eseguire operazioni di stampa o operazioni taglia e incolla degli elementi per salvare i dati di Controllo versione al momento della visualizzazione.

Nel riquadro delle informazioni di Controllo delle versioni sono visualizzati i seguenti campi:

- Categoria
- Data
- Registro
- Attributo
- Nuovo valore
- Valore precedente
- Modificato da
- MDR

Nota: il registro visualizza soltanto gli *aggiornamenti* di attributo relativi agli elementi della configurazione creati in versioni precedenti di CA SDM o CA CMDB; non visualizza i valori attributo dell'elemento della configurazione iniziale. Le relazioni create in versioni precedenti di CA SDM o CA CMDB non includono informazioni sulla cronologia di audit e non sono visualizzate nel registro.

Filtraggio del registro

È possibile filtrare il registro mediante l'immissione di una semplice stringa nel campo Filtro. Il filtro non è sensibile alla distinzione tra maiuscole e minuscole. Se la stringa del filtro è contenuta in qualsiasi punto di una riga del registro, tale riga viene visualizzata. Nei filtri non vengono utilizzati caratteri speciali o caratteri jolly. Le righe del registro corrispondenti ai criteri del filtro vengono visualizzate, mentre quelle non corrispondenti vengono nascoste.

Non occorre premere Invio o Aggiorna per aggiornare la visualizzazione. La visualizzazione del registro viene filtrata ogni volta che si preme un tasto. Ciò vale per tutti i campi, ad esempio Data, Registro, Attributo, Valore precedente, Nuovo valore, MDR e Nome.

Visualizzazione della cronologia degli elementi di configurazione

È possibile visualizzare la cronologia di un elemento della configurazione.

Per visualizzare la cronologia di un elemento della configurazione:

1. Individuare e aprire l'elemento di configurazione.

   Viene visualizzata la pagina Dettagli elemento della configurazione.

2. Fare clic sulla scheda Controllo delle versioni.

   Viene visualizzata la pagina Controllo delle versioni.

3. Fare clic su Mostra registro.

   Viene visualizzata la cronologia dell'elemento di configurazione.

   Nota: l'opzione Mostra registro ignora le selezioni del riquadro sinistro.

Stampa del registro di un elemento della configurazione

È possibile stampare il registro di un elemento della configurazione.

Per stampare il registro di un elemento di configurazione procedere come segue

1. Selezionare un elemento di configurazione e fare clic sulla relativa scheda Controllo delle versioni.
2. Fare clic sul collegamento Visualizza registro.
3. (Facoltativo) Immettere il criterio di filtro desiderato per nascondere/visualizzare le righe del registro.
4. Fare clic su Stampa.

   Viene visualizzata una finestra già predisposta per la stampa. Viene visualizzato il report Controllo delle versioni dell'elemento di configurazione.

5. Nella finestra del browser Web fare clic su File e Stampa per stampare una copia del report.

   Il testo formattato viene inviato alla stampante predefinita.

Supporto dell'esportazione in formato CSV

È possibile esportare i contenuti del registro CA CMDB in un file di formato CSV (Comma Separated Value) importabile in applicazioni o strumenti di reporting di terze parti. L'esportazione si basa sul contenuto attualmente visualizzato, che può essere filtrato o meno.

Ulteriori informazioni:

Esporta dati (a pagina 628)

Registri integrati di CA SDM e CA APM

Oltre alle modifiche apportate utilizzando le funzionalità di CA CMDB, il registro dell'elemento della configurazione include gli eventi di aggiornamento derivanti dalle attività del ticket delle modifiche di CA SDM e dagli aggiornamenti di CA APM.

Ulteriori informazioni:

CA APM Integrazione (a pagina 610)

Avvio nel contesto MDR e identificazione dell'origine

CA CMDB offre una funzione di avvio nel contesto che consente di avviare direttamente dal registro nel provider di dati MDR una voce specifica del registro dell'elemento della configurazione. È possibile eseguire l'avvio in contesto per la specifica del Cambiamento. Questa funzione di avvio consente di effettuare le seguenti azioni:

- Tenere traccia delle modifiche apportate agli attributi per l'MDR di origine, quando MDR ha utilizzato i tag <mdr_name> <mdr_class> e <federated_asset_id> in GRLoader.

  Nota: per ulteriori informazioni, *consultare la Guida di riferimento tecnico CA CMDB*.

- Rilevare quando è in corso l'aggiornamento di un attributo dell'elemento di configurazione da parte di più MDR. Questa situazione si verifica quando più MDR collaborano indipendentemente ai dati di definizioni di elementi di configurazione.
- Individuare l'MDR che costituisce l'origine autorizzata.

Nota: le voci del registro create in CA SDM o nelle versioni precedenti di CA CMDB non contengono le informazioni di avvio MDR nel contesto. Inoltre, CA Cohesion ACM fornisce le informazioni di avvio nel contesto MDR per la maggior parte di tutti gli attributi e relazioni, ma non per tutti.

Nomi degli attributi

I nomi degli attributi visualizzati nel registro corrispondono ai nomi degli attributi visualizzati nell'interfaccia utente e non riflettono il nome interno dell'oggetto. Ad esempio, CA CMDB visualizza “Tipo di manutenzione” invece di “mtce_type”.

Registrazione delle famiglie e degli attributi personalizzati

È necessario specificare i nuovi attributi MDR e i trigger di audit per abilitare la registrazione delle famiglie e degli attributi personalizzati. Se si creano nuove famiglie o nuovi attributi, è necessario creare anche file di metadati per specificare il nome attributo leggibile da visualizzare nel registro. In caso contrario verranno visualizzati i nomi interni degli oggetti.

Nota: per ulteriori informazioni, consultare Estensione di CA CMDB nella *Guida all'amministrazione*.

Creazione di un'attività cardine

È possibile creare un'attività cardine dall'interfaccia utente o utilizzando GRLoader.

Per creare un'attività cardine dall'interfaccia utente procedere come segue

1. Selezionare un elemento di configurazione e fare clic sulla relativa scheda Controllo delle versioni.
2. Fare clic su Crea attività cardine.
3. Immettere del testo descrittivo per l'attività cardine. Fare clic su Salva.

   La finestra Crea cardine viene chiusa.
4. Selezionare Visualizza, quindi Aggiorna.

   La visualizzazione di base visualizza una nuova snapshot, con la data e l'ora correnti, che rappresenta l'attività cardine appena creata. Se si passa alla visualizzazione Cardine, vengono visualizzate solo le snapshot con i nomi assegnati. Le attività cardine vengono visualizzate in una sequenza data/ora decrescente, con quella più recente visualizzata nella parte superiore.

Per creare un'attività cardine utilizzando GRLoader procedere come segue

1. Aggiungere il tag <milestone> all'XML per tale elemento della configurazione.
2. Vengono applicate le stesse regole di riconciliazione dell'associazione di un'attività cardine con un elemento della configurazione.

   Nota: il valore del tag milestone corrisponde all'etichetta associata a tale attività cardine.
3. Salvare e chiudere il file XML per l'elemento della configurazione.

   L'attività cardine viene creata.

Nota: per ulteriori informazioni, *vedere la Guida di riferimento tecnico CA CMDB*.

Esempio: Utilizzo di GRLoader per creare un cardine

Nel seguente esempio su GRLoader viene creata l'attività cardine **Fine anno fiscale 2008**.

```
<ci>
<name>server1 </name>
<milestone>Fine anno fiscale 2008</milestone>
<ci>
```

Creazione di un elemento di configurazione standard

Un elemento della configurazione standard viene creato come qualsiasi altro elemento della configurazione.

Per creare un elemento di configurazione standard nell'interfaccia utente procedere come segue

1. Selezionare Crea nuovo elemento configurazione nel menu File.
2. Selezionare la famiglia che si intende utilizzare per il nuovo elemento della configurazione standard.
3. Definire gli attributi, come con qualsiasi comune elemento della configurazione.

   L'elemento della configurazione standard viene creato.

Nota: qualsiasi elemento della configurazione può fungere da elemento della configurazione standard, tuttavia è necessario tenere presente quanto segue:

- Un elemento della configurazione standard deve seguire una convezione di denominazione affinché non possa essere confuso con gli elementi della configurazione standard normali.
- Un elemento della configurazione standard può agire solo come linea di base per gli elementi della configurazione appartenenti alla sua stessa famiglia.
- A un elemento della configurazione standard *non* è possibile assegnare valori per nessuno degli attributi utilizzati nella riconciliazione, come ad esempio Indirizzo MAC, Numero di serie, ID elemento della configurazione alternativo, DNS e così via.
- Poiché gli elementi della configurazione standard non possono essere distinti dai normali elementi della configurazione, essi vengono visualizzati nel contatore e inclusi nel conteggio del numero totale di elementi della configurazione.
- È preferibile che un elemento della configurazione standard non rappresenti alcuna istanza reale di un oggetto di business.

Assegnazione di un elemento della configurazione standard a un elemento della configurazione

È possibile assegnare un elemento della configurazione standard a un elemento della configurazione utilizzando la pagina Dettagli elementi della configurazione. È possibile assegnare un elemento della configurazione standard a un elenco di elementi della configurazione o utilizzando Modifica in elenco.

Per assegnare un elemento della configurazione standard di una famiglia a un elemento della configurazione utilizzando la pagina Dettagli elementi della configurazione

1. Selezionare un elemento di configurazione e fare clic su Modifica.

   Viene visualizzata la pagina Aggiorna elemento della configurazione.

2. Fare clic sull'icona visualizzata accanto al campo Elemento di configurazione standard.

   Viene visualizzato l'Elenco elemento di configurazione.

3. Selezionare l'elemento di configurazione da utilizzare come elemento di configurazione standard. Fare clic su Salva.

   L'elemento di configurazione standard viene assegnato.

Per assegnare gli elementi di configurazione standard a un elenco di elementi di configurazione utilizzando la funzione Modifica in elenco

1. Dalla scheda Contatore o Amministrazione, specificare il filtro di ricerca per visualizzare uno o più elementi della configurazione nell'elenco dei dettagli, quindi fare clic su Cerca.

   Vengono elencati gli elementi di configurazione corrispondenti ai criteri di ricerca.

2. Fare clic sul pulsante Modifica in elenco nella parte superiore destra dei risultati dell'elenco.

   Vengono visualizzati i controlli di Modifica in elenco dell'elemento di configurazione.

3. Selezionare anche una riga contenente l'elemento di configurazione a cui assegnare l'elemento di configurazione.

   La riga viene visualizzata con un colore evidenziato.

4. Fare clic sull'icona visualizzata accanto al campo Elemento di configurazione standard.

   Viene visualizzato l'Elenco elemento di configurazione.

5. Selezionare l'elemento di configurazione da utilizzare come elemento di configurazione standard. Fare clic su Salva per aggiornare il singolo elemento di configurazione o su Modifica tutto per modificare tutti gli elementi di configurazione presenti nell'elenco.

   L'elemento di configurazione standard viene assegnato a un singolo elemento di configurazione (impostazione Salva) o a tutti gli elementi di configurazione (impostazione Modifica tutto)

Nota: qualsiasi elemento della configurazione può fungere da elemento della configurazione standard, tuttavia è necessario tenere presente quanto segue:

- Un elemento della configurazione standard deve seguire una convezione di denominazione affinché non possa essere confuso con gli elementi della configurazione standard normali.
- Un elemento della configurazione standard può agire solo come linea di base per gli elementi della configurazione appartenenti alla sua stessa famiglia.
- A un elemento della configurazione standard *non* è possibile assegnare valori per nessuno degli attributi utilizzati nella riconciliazione, come ad esempio Indirizzo MAC, Numero di serie, ID elemento della configurazione alternativo, DNS e così via.
- Poiché gli elementi della configurazione standard non possono essere distinti dai normali elementi della configurazione, essi vengono visualizzati nel contatore e inclusi nel conteggio del numero totale di elementi della configurazione.

È preferibile che un elemento della configurazione standard non rappresenti alcuna istanza reale di un oggetto di business.

Assegnazione di un elemento di configurazione standard a un elemento di configurazione utilizzando GRLoader

Per assegnare un elemento della configurazione standard a un elemento della configurazione, includere il tag <standard_ci> nella descrizione dell'elemento.

Nota: per ulteriori informazioni, *vedere la Guida di riferimento tecnico CA CMDB*.

Esempio: Assegnazione di un elemento della configurazione standard a un elemento della configurazione

Se si dispone di una configurazione di workstation standard memorizzata in un elemento della configurazione denominato **configurazione workstation standard** , è possibile assegnare tale elemento della configurazione a una determinata workstation utilizzando GRLoader per caricare il seguente codice XML:

```
<ci>
        <name>Workstation di Joe</name>
        <class>Server</class>
        <standard_ci> configurazione workstation standard</standard_ci>
<ci>
```

Uso della visualizzazione di base

È possibile selezionare le snapshot nella visualizzazione di base o avanzata; gli stessi tipi di dati di versione possono essere visualizzati in entrambi i modi. La visualizzazione di base consente di visualizzare con facilità lo stato di un elemento della configurazione.

Per utilizzare la visualizzazione base per lo stato di un elemento della configurazione

1. Aprire l'elemento di configurazione nell'interfaccia utente e fare clic sulla scheda Controllo delle versioni.

   Gli snapshot esistenti vengono elencati sul lato sinistro della pagina.

2. Selezionare un tipo di snapshot dall'elenco a discesa Tipo di snapshot:

   Nota: se per l'elemento della configurazione focale si seleziona un elemento della configurazione standard, tale elemento viene visualizzato in cima all'elenco di snapshot o cardini ed è contrassegnato da un indicatore "elemento della configurazione standard" a destra del nome dell'elemento. Facendo clic su un elemento della configurazione standard, vengono visualizzati gli attributi dell'elemento della configurazione standard e non dell'elemento della configurazione focale.

   Snapshot

   Elenca tutte le snapshot dell'elemento della configurazione identificate sulla base di data/ora e l'elemento della configurazione standard. Questa è l'opzione predefinita.

Cardine

Elenca tutte le attività cardine definite dall'utente e l'elemento della configurazione standard.

Nel riquadro destro viene visualizzato lo stato dell'elemento della configurazione.

L'area contenente testo informativo visualizzata nella parte inferiore fornisce informazioni sull'elemento corrente sul quale si sta passando il mouse. Passando con il mouse su una snapshot, un'attività cardine o un elemento della configurazione standard, vengono visualizzate informazioni sulla data e ora di creazione e sul tipo di snapshot.

Nota: è possibile selezionare due o più snapshot, attività cardine o elementi della configurazione standard per il confronto.

Utilizzare la visualizzazione avanzata

È possibile scegliere snapshot nella visualizzazione di base o avanzata; gli stessi tipi di dati di versione possono essere visualizzati in entrambi i modi. La visualizzazione avanzata consente di visualizzare le snapshot in base al tipo di attributo, al valore e alla data/ora. È inoltre possibile eseguire qualsiasi tipo di confronto con attributi, attività cardine o elementi della configurazione standard. Una struttura gerarchica mostra una cartella per ciascun attributo dell'elemento della configurazione, e ogni cartella di attributo contiene una cronologia dei valori dell'attributo. La gerarchia è organizzata nel seguente modo:

```
Principale
     Nome attributo
          Valore attributo 1
          Valore attributo 2
```

Questa gerarchia consente di visualizzare immediatamente la cronologia di valori unici per qualsiasi attributo specifico.

Per utilizzare la visualizzazione avanzata

1. Aprire l'elemento di configurazione nell'interfaccia utente e fare clic sulla scheda Controllo delle versioni.

   Gli snapshot esistenti vengono elencati sul lato sinistro della pagina.

2. Fare clic su Avanzate.

   Selezione avanzata mostra una gerarchia di cartelle.

3. Individuare la cartella contenente le informazioni che si desidera visualizzare e fare clic su di essa:

   Data

   Elenca le snapshot in base alla data/ora, in modo identico alla visualizzazione di base. Le snapshot possono essere suddivise ulteriormente in base all'anno/mese se ne sono presenti almeno 30 per l'elemento della configurazione. L'elemento della configurazione standard è elencato anche in questa cartella se è stata assegnata all'elemento della configurazione focale.

   Cardine

   Elenca tutte le attività cardine definite dall'utente, in modo identico alla visualizzazione di base. L'elemento della configurazione standard è elencato anche in questa cartella se è stata assegnata all'elemento della configurazione focale.

   Gli attributi degli elementi di configurazione standard vengono visualizzati come nodi della struttura con un "elemento di configurazione standard". I valori dell'elemento della configurazione standard vengono visualizzati solo per gli attributi che possiedono un valore per l'elemento della configurazione standard; non vengono visualizzati per gli attributi che non presentano tale valore impostato.

   Relazione

   Contiene tutte le relazioni (passate e presenti) relative all'elemento della configurazione. La gerarchia delle cartelle indica quanto segue:

```
Relazione
    Tipo relazione
        Elemento di configurazione partner
            Stato e data
```

Tipo relazione specifica il tipo di relazione, ad esempio "è contenuto da", "ospita" o "comunica con".

Elemento della configurazione partner è il nome dell'elemento della configurazione associato alla relazione.

Stato e Data specificano lo stato della relazione nella data e all'ora specificate. I valori di stato includono i seguenti:

- Relazione creata — lo stato dell'elemento della configurazione nel momento in cui la relazione è stata creata.
- Relazione terminata — l'elemento della configurazione non è più interessato dalla relazione. La relazione esiste ancora dalla parte del partner, tuttavia l'elemento di configurazione con stato attivo non è più interessato.
- Relazione eliminata — la relazione è stata contrassegnata come eliminata.
- Relazione modificata — la relazione è stata riattivata dopo essere stata eliminata.
- New Partner and Type—Il lato partner della relazione è stato assegnato a un nuovo elemento della configurazione e contemporaneamente è stato modificato il tipo di relazione.
- Nuovo tipo di relazione — il tipo di relazione tra due elementi della configurazione è stato modificato.
- Elemento della configurazione partner assegnato — la parte del partner della relazione è stata modificata.

4. Fare clic su un valore attributo.

   Viene visualizzato lo stato completo dell'elemento della configurazione corrispondente al momento in cui il valore attributo è stato impostato.

Esempio: Utilizzo della visualizzazione Avanzata per mostrare gli attributi relativi allo spazio su disco

Nel seguente esempio, Selezione avanzata mostra che lo spazio su disco è stato aumentato da 10 a 20 poi a 100 GB.

```
Principale
      Spazio su disco
            10 GB
            20 GB
            100 GB
```

Facendo clic su un valore è possibile vedere quando la modifica ha avuto luogo, lo stato degli altri attributi al momento in cui è avvenuta e il numero della richiesta di modifica aperta quando lo spazio su disco è stato aumentato.

Visualizzazione dettagli snapshot

È possibile visualizzare le snapshot nella visualizzazione di base o avanzata. Ad esempio, la visualizzazione di base consente di visualizzare la snapshot di un Cambiamento non pianificato dell'elemento della configurazione.

Per visualizzare i dettagli della snapshot

1. Aprire l'oggetto nell'interfaccia utente e fare clic sulla scheda Controllo delle versioni.

   Nella parte sinistra della pagina viene visualizzato un elenco di tutte le snapshot esistenti.

2. Fare clic su una snapshot.

   I dettagli vengono visualizzati nel riquadro destro delle visualizzazioni di base e avanzata. Se si seleziona un singolo elemento, nel riquadro destro vengono visualizzate le informazioni relative alla snapshot, il cardine o l'elemento della configurazione standard selezionato.

   I dati visualizzati includono i seguenti dettagli e indicatori:

   Nascondi valori vuoti

   Consente il filtraggio di campi dati vuoti. Se non si seleziona questa opzione, vengono visualizzati tutti gli attributi degli elementi della configurazione.

   Testo del campo Valore in grassetto

   Indica che un attributo o una relazione sono stati modificati dalla creazione dell'ultima snapshot. Quando si visualizzano i dettagli relativi a un elemento di configurazione, tutti i valori vengono visualizzati in grassetto.

   Valore

   Se si passa il mouse sul valore, viene visualizzato il valore precedente dell'attributo e le informazioni temporali relative all'ultima modifica. Le informazioni compaiono nell'area di testo presente nella parte inferiore della scheda Controllo delle versioni.

   Valore “(vuoto)”

   Indica se è stato cancellato un valore precedente.

Categoria relazione

Mostra informazioni sulla relazione, compresi il tipo e l'elemento della configurazione partner.

Avvio nel contesto MDR e identificazione dell'origine

Offre l'avvio nel contesto a un MDR provider dalla voce dettaglio dell'elemento della configurazione.

Nota: gli elementi della configurazione creati in USDK o nelle versioni precedenti di CA CMDB potrebbero non includere le informazioni MDR e sull'autore della modifica. Inoltre, CA Cohesion ACM fornisce le informazioni di avvio nel contesto MDR per la maggior parte degli attributi e relazioni, ma non per tutti.

Tiene traccia delle modifiche agli attributi per l'MDR fonte.

Rilava quando è in corso l'aggiornamento di un attributo di un elemento della configurazione da parte di uno o più MDR. Questa situazione si verifica quando più MDR collaborano indipendentemente ai dati di definizioni di elementi di configurazione.

Consente di identificare l'MDR che sta agendo come origine autorizzata.

Visualizzazione dello stato di un elemento della configurazione in una determinata data (visualizzazione di base)

È possibile utilizzare la visualizzazione di base per esaminare lo stato di un elemento della configurazione in una data specifica.

Per visualizzare lo stato di un elemento della configurazione in una data specifica

1. Selezionare un elemento della configurazione e accedere alla relativa pagina Dettagli elementi della configurazione.
2. Fare clic sulla scheda Controllo delle versioni.

   Viene mostrata la visualizzazione di base dell'elemento della configurazione.
3. Selezionare una data.

   La parte destra del display mostra lo stato dell'elemento della configurazione alla data selezionata.

Visualizzazione dello stato di un elemento della configurazione in una determinata data (visualizzazione avanzata)

È possibile utilizzare Selezione avanzata per visualizzare lo stato di un elemento della configurazione in una data specifica.

Per visualizzare lo stato di un elemento della configurazione in una data specifica

1. Selezionare un elemento della configurazione e accedere alla relativa pagina Dettagli elementi della configurazione.
2. Fare clic sulla scheda Controllo delle versioni, quindi su Avanzate.

   Viene visualizzata la struttura di selezione avanzata.
3. Espandere la cartella Data.
4. Selezionare la data per cui si desidera visualizzare l'elemento della configurazione.

   Viene visualizzato lo stato dell'elemento di configurazione in tale data.

Avvio dell'MDR che imposta un attributo

Se la cronologia di un elemento della configurazione fa riferimento a un MDR, è possibile lanciarne uno per visualizzare i dettagli dell'elemento della configurazione stesso.

Per avviare un MDR al fine di visualizzare i dettagli relativi all'elemento della configurazione

1. Selezionare un elemento della configurazione e accedere alla relativa pagina Dettagli elementi della configurazione.
2. Fare clic sulla scheda Controllo delle versioni.
3. Fare clic su Visualizza registro o selezionare la snapshot o l'attività cardine dell'elemento della configurazione che si desidera visualizzare.
4. Selezionare la riga di attributo su cui si desidera ottenere informazioni.
5. Se la cronologia dell'elemento della configurazione fa riferimento a un MDR, fare clic sul collegamento MDR.

   L'MDR fornitore mostra ulteriori dettagli sull'elemento della configurazione.

Stampa di una snapshot

È possibile stampare una snapshot a partire da una data selezionata.

Procedere come descritto di seguito:

1. Selezionare l'oggetto e fare clic sulla scheda Controllo delle versioni.
2. Selezionare la visualizzazione di base.
3. Selezionare Snapshot dall'elenco a discesa Tipo di snapshot.
4. Selezionare la data nell'elenco delle date visualizzato sulla sinistra.
5. Fare clic su Stampa.

   Viene visualizzata una finestra già predisposta per la stampa contenente il report Controllo delle versioni per l'oggetto.
6. Utilizzare la finestra del browser Web per fare clic su File e quindi su Stampa per stampare il report.

   Il testo formattato viene inviato alla stampante predefinita.

Stampa di un cardine di un elemento della configurazione

È possibile stampare un'attività cardine di un elemento della configurazione in una data selezionata.

Per stampare un cardine di un elemento della configurazione in una data selezionata procedere come segue:

1. Selezionare un elemento di configurazione e fare clic sulla relativa scheda Controllo delle versioni.
2. Selezionare un'attività cardine nella visualizzazione di base o avanzata.
3. Fare clic su Stampa.

   Viene visualizzata una finestra già predisposta per la stampa che visualizza il report Controllo delle versioni per l'elemento della configurazione.
4. Utilizzare la finestra del browser Web per fare clic su File e quindi su Stampa per stampare il report.

   Il testo formattato viene inviato alla stampante predefinita.

Esporta dati

La pagina di controllo delle versioni per l'esportazione in formato CSV consente di esportare la snapshot e le informazioni del registro in formato CSV. I dati vengono visualizzati in una pagina di esportazione. I dati formattati corrispondono alla visualizzazione ottenuta con le righe visualizzate su linee separate contenenti valori in colonne separati da virgola racchiusi tra virgolette. Gli elementi formattati per l'esportazione sono il tipo di filtraggio e i dati di confronto selezionati nella scheda relativa al controllo versioni.

Per esportare i dati dell'elemento della configurazione

1. Selezionare un oggetto e fare clic sulla scheda Controllo delle versioni.
2. Fare clic sulla visualizzazione dell'elemento della configurazione desiderata.

   Ad esempio, fare clic su Mostra registro, su un confronto di snapshot, su un cardine (solo elemento della configurazione), eccetera.
3. Fare clic su Esporta.

   Viene visualizzata la pagina Esporta registro a CSV per elemento della configurazione.
4. Utilizzare l'opzione Seleziona tutto (dal menu di scelta rapida o tramite i tasti di scelta rapida).
5. Utilizzare i comandi Copia e Incolla per trasferire i dati dalla pagina formattata in un file CSV o un'applicazione di terze parti. È ad esempio possibile esportare i dati in un foglio di calcolo Excel

   I dati vengono esportati.

Modifiche e snapshot della famiglia di un elemento di configurazione

Le modifiche relative alla famiglia possono avere effetti su una snapshot o un elemento della configurazione.

Una snapshot include i seguenti tipi di attributi:

- Attributi comuni
- Attributi specifici della famiglia

Quando si modifica la famiglia di un elemento della configurazione, si verifica quanto segue:

- Gli attributi specifici della famiglia associati all'elemento della configurazione vengono modificati.
- I dettagli della snapshot rispecchiano la situazione della famiglia al momento della creazione della snapshot.

La famiglia di un elemento di configurazione determina gli attributi posseduti dall'elemento di configurazione. Se si modifica un attributo *specifico della famiglia* dopodiché si modifica la famiglia dell'elemento della configurazione, il risultato è un elemento della configurazione che non possiede più l'attributo *specifico della famiglia* modificato. La modifica della famiglia di un elemento della configurazione non ha conseguenze sugli attributi *comuni* di quest'ultimo.

Esempio: Modifica della famiglia associata a un elemento della configurazione

Questo esempio mostra l'effetto delle modifiche alla famiglia di un elemento della configurazione su una snapshot dello stesso.

Ora	Stato/Modifiche
0	L'elemento di configurazione è nella famiglia1.
1	È stato modificato il valore di un attributo specifico della famiglia1.
2	Sono stati modificati diversi valori di attributo comuni.
3	La famiglia dell'elemento di configurazione è stata modificata da famiglia1 a famiglia2. Quando questo si verifica, tutti gli attributi specifici della famiglia1 non sono più disponibili per l'elemento di configurazione.
4	È stato modificato il valore di un attributo specifico della famiglia2.
5	Sono stati modificati diversi attributi comuni.
6	La famiglia dell'elemento della configurazione è stata nuovamente modificata in famiglia1. Quando questo si verifica, tutti i valori degli attributi specifici della famiglia1 non sono più disponibili per l'elemento della configurazione, tuttavia vengono ripristinati tutti i valori degli attributi specifici della famiglia1.
7	Sono stati modificati diversi attributi comuni.
8	È stato modificato il valore di un attributo specifico della famiglia1.

Nell'esempio, una snapshot creata all'ora=7 non contiene le informazioni provenienti dalle modifiche eseguite alle ore 3 o 4. Queste modifiche rappresentano le modifiche degli attributi specifici della famiglia2.

Confronto di snapshot (visualizzazione di base)

È possibile confrontare due o più snapshot, attività cardine o elementi della configurazione standard.

Per confrontare snapshot, attività cardine o elementi della configurazione standard

1. Selezionare un elemento della configurazione e accedere alla relativa pagina Dettagli elementi della configurazione.
2. Fare clic sulla scheda Controllo delle versioni.
3. Selezionare un'attività cardine o una snapshot dall'elenco a discesa Tipo di snapshot.

   Vengono elencate le attività cardine e le snapshot.
4. Selezionare una o più snapshot, attività cardine o elementi della configurazione standard.

   La visualizzazione di confronto mostra i seguenti risultati:

   - Una colonna mostra la differenza tra snapshot o attività cardine.
   - In ciascuna riga vengono visualizzati i valori degli attributi relativi alle snapshot selezionate.
   - Vengono visualizzati solo gli attributi che presentano differenze. La data è sempre visualizzata a meno che le snapshot non siano identiche.
   - I confronti degli elementi della configurazione standard non sono specifici dell'ora, pertanto i campi Data visualizzano la voce **Elemento della configurazione standard**.
   - I risultati del confronto possono essere stampati o esportati in un file con formato CSV.

Confronto tra snapshot (visualizzazione avanzata)

È possibile confrontare due o più snapshot, attività cardine o elementi della configurazione standard.

Per confrontare snapshot, attività cardine o elementi della configurazione standard nella visualizzazione avanzata

1. Selezionare un elemento della configurazione e accedere alla relativa pagina Dettagli elementi della configurazione.
2. Fare clic sulla scheda Controllo delle versioni, quindi su Avanzate.

   Selezione avanzata visualizza l'elemento della configurazione.
3. Nella gerarchia delle cartelle, individuare il valore che si desidera utilizzare per il confronto della snapshot.
4. Selezionare un valore per ciascun confronto di snapshot.

   Viene visualizzato il confronto per l'elemento della configurazione, ad esempio un confronto tra snapshot basato sui valori della cartella selezionati.

   La visualizzazione di confronto mostra i seguenti risultati:

   - Una colonna mostra la differenza tra snapshot o attività cardine.
   - In ciascuna riga vengono visualizzati i valori degli attributi relativi alle snapshot selezionate.
   - Vengono visualizzati solo gli attributi che presentano differenze. La data è sempre visualizzata a meno che le snapshot non siano identiche.
   - I confronti degli elementi della configurazione standard non sono specifici dell'ora, pertanto i campi Data visualizzano la voce **Elemento della configurazione standard**.
   - I risultati del confronto possono essere stampati o esportati in un file con formato CSV.

Nota: nella visualizzazione avanzata, due elementi della configurazione possono avere una relazione a cui non sia stato assegnato un tipo. Ad esempio, gli elementi della configurazione creati da CA NSM. Tali nodi della relazione sono identificati come (vuoti).

Gestione delle modifiche in CA SDM

I dati del controllo delle versioni vengono generati in modo automatico per ciascun elemento della configurazione associato a un ticket delle modifiche di CA Service Desk. Mentre il ticket delle modifiche passa da aperto ad attivo, quindi a risolto e a chiuso, viene creata una snapshot per ciascuno degli elementi della configurazione associati. Il controllo delle versioni consente di effettuare le operazioni seguenti:

- Confrontare lo stato dell'elemento della configurazione con il relativo elemento della configurazione standard in qualsiasi punto di un ciclo di vita di gestione delle modifiche.
- Garantire che l'elemento della configurazione sia conforme e identificare gli attributi che necessitano correzioni.
- Eseguire confronti tra gli stati dell'elemento della configurazione in qualsiasi momento del ciclo di vita dell'ordine di cambiamento, ma anche in qualsiasi data o ora intermedie.
- Visualizzare l'andamento in ogni fase della modifica, comprese tutte le attività cardine.

L'integrazione tra CA Service Desk e CA CMDB è illustrata dimostrando come è possibile controllare le modifiche eseguite durante il ciclo di vita della gestione dei servizi di un elemento della configurazione. In questo esempio viene utilizzata una richiesta di cambiamento per aggiornare componenti di un server hardware.

Per creare un ordine di cambiamento e associarlo a un elemento della configurazione procedere come segue

1. Creare un ticket di cambiamento di CA Service Desk facendo clic su File, Nuovo ordine di cambiamento.
2. Immettere le informazioni della richiesta di cambiamento e il riepilogo dell'ordine, ad esempio: Aggiornare disco rigido a 500 GB.
3. Fare clic sulla scheda Elementi della configurazione, quindi su Aggiorna elementi della configurazione.
4. Specificare i criteri di ricerca dell'elemento della configurazione, ad esempio il nome del server hardware, quindi fare clic su Cerca.
5. Nel modulo Aggiorna elementi della configurazione interessati selezionare gli elementi della configurazione associati al ticket di cambiamento (ad esempio, il server hardware del passaggio 4), e aggiungerli all'elenco Elementi della configurazione interessati. Fare clic su OK.
6. Salvare la richiesta di cambiamento.

Per apportare le modifiche procedere come segue

1. Eseguire le modifiche dell'elemento della configurazione. Ad esempio, eseguire l'installazione del disco rigido sul computer fisico, quindi aggiornare l'attributo Capacità disco per l'elemento della configurazione server hardware.
2. Chiudere la richiesta di cambiamento.
3. Per assicurarsi che le modifiche siano state completate, visualizzare l'elemento della configurazione, fare clic sulla scheda Controllo delle versioni e confrontare le snapshot dell'elemento prima e dopo il cambiamento.

   Confrontando lo stato dell'elemento della configurazione dall'apertura dell'ordine di cambiamento alla sua chiusura, si nota che la capacità del disco rigido del server hardware era di 100 GB prima del cambiamento e di 500 GB dopo il cambiamento, e vengono indicati data e ora dei cambiamenti. È inoltre possibile vedere qualsiasi altro attributo che è stato modificato tra l'ora di apertura e chiusura.

Visualizzazione degli attributi degli elementi della configurazione in altri prodotti CA

È possibile utilizzare la pagina Common Asset Viewer per visualizzare attributi di elementi della configurazione in altri prodotti CA.

Per visualizzare gli attributi degli elementi della configurazione in altri prodotti CA

1. Individuare e aprire l'elemento della configurazione.
2. Fare clic su Visualizzatore asset.

   Viene visualizzata la pagina Common Asset Viewer.
3. Fare clic sui collegamenti della scheda Risorse possedute per individuare le informazioni sugli attributi da altri prodotti CA.
4. Fare clic su Chiudi finestra per continuare.

   Sono stati visualizzati attributi di elementi della configurazione di altri prodotti CA.

Utilizzo di Visualizzatore CMDBf

In CA SDM è disponibile il Visualizzatore CMDBf che consente di visualizzare i risultati della federazione di elementi della configurazione nei repository dati di gestione MDR. Da una pagina Dettagli elemento della configurazione (oppure nel menu di scelta rapida visualizzato facendo clic con il pulsante destro del mouse su un elemento della configurazione in un elenco di elementi della configurazione), fare clic su Visualizzatore CMDBf per visualizzare contemporaneamente gli attributi elemento della configurazione di CMDB federati e MDR. Nella vista federata è possibile fare clic sul pulsante Recupera per aggiornare le informazioni da qualsiasi MDR federato. Per una migliore leggibilità, i file metadata CA CMDB possono riconciliare i nomi di attributi MDR e i nomi di attributi CA CMDB.

Nota: questa funzionalità richiede repository dati di gestione MDR che supportano Query. Per configurare i risultati nella vista federata, è necessario configurare gli endpoint CMDBf MDR. Per ulteriori informazioni, consultare la *Guida all'implementazione*.

Se l'elemento della configurazione non dispone di dati federati, il visualizzatore mostra solo attributi CA CMDB.

Visualizzatore CMDB

CA SDM consente di allineare i componenti IT (*elementi della configurazione*) con i servizi aziendali. CA CMDB definisce *relazioni* tra gli elementi della configurazione, ad esempio se si utilizza un gruppo di elementi della configurazione per offrire un servizio aziendale. CMDB Visualizer consente di ottenere una panoramica completa delle relazioni tra gli elementi della configurazione offrendo funzionalità per la gestione delle relazioni. Gli *elementi della configurazione con stato attivo* (ovvero qualsiasi elemento della configurazione desiderato) consente di utilizzare il visualizzatore per mostrare fino a nove livelli di elementi della configurazione correlati.

Nota: (solo configurazione Disponibilità avanzata) Se il visualizzatore effettua una richiesta al server durante la fase di disattivazione del server applicazioni, viene visualizzato il messaggio seguente:

Arresto del server CMDB Visualizer pianificato per la manutenzione tra xx:xx. Salvare le modifiche ed effettuare la disconnessione.

È possibile nascondere la casella del messaggio, che continua a essere mostrato nel pannello in alto durante il periodo di disattivazione. Se la disattivazione del server viene annullata, verrà visualizzato un messaggio di avviso.

Per definire le relazioni tra gli elementi della configurazione, CA utilizza un modello di tipo provider/dipendente. Tutti gli elementi della configurazione che contribuiscono a un servizio aziendale fungono da *provider* di tale servizio (che a sua volta è il *dipendente*). Analogamente, i provider possono essere *dipendenti* di altri elementi della configurazione. Il visualizzatore consente di effettuare le analisi provider/dipendente seguenti:

Sfoglia

Mostra una visualizzazione non filtrata di tutti gli elementi della configurazione.

Analisi impatto

Viene avviata a livello di un elemento della configurazione con stato attivo (provider) ed esegue la ricerca degli elementi dipendenti.

Causa principale

Viene avviata a livello di un servizio aziendale (dipendente) e visualizza tutti gli elementi della configurazione provider di tale servizio.

Elementi della configurazione causa-effetto

Combina l'analisi di impatto e la causa principale in un'unica ricerca.

Tieni traccia della relazione

Consente di visualizzare tutte le relazioni possibili in base ai livelli. Se si seleziona un solo elemento della configurazione, questo filtro mostra la visualizzazione Sfoglia.

Percorso più breve

Consente di visualizzare la catena di relazioni più breve in base ai livelli.

CMDB Visualizer consente di effettuare le azioni seguenti:

- Visualizzare più livelli di elementi della configurazione da una visualizzazione grafica configurabile
- Monitorare o annullare lo stato di avanzamento del rendering
- Effettuare una ricerca utilizzando criteri flessibili
- Filtrare in base a famiglie di elementi della configurazione, tipi di relazione e altri attributi
- Visualizzare relazioni tra elementi della configurazione
- Tracciare una relazione tra due elementi della configurazione
- Visualizzare una catena di dipendenze
- Richiamare CA CMDB direttamente dal visualizzatore

- Visualizzare attributi e proprietà degli elementi della configurazione
- Salvare metadati di grafici
- Stampare il layout grafico
- Cercare un elemento della configurazione specifico in un grafico visualizzato
- Creare un elemento della configurazione (in base al ruolo)
- Creare nuove relazioni tra elementi della configurazione (in base al ruolo)
- Utilizzare Blocco note per annotare gli elementi della configurazione principali
- Visualizzare lo stato degli elementi della configurazione
- Nascondere o visualizzare un elemento della configurazione nel layout del visualizzatore
- Protezione dei dati basata sui ruoli
- Avviare MDR esterni
- Visualizzare informazioni della Guida in linea per le funzionalità del visualizzatore

Ulteriori informazioni:

Analisi della causa principale (a pagina 637)
Amministrazione del visualizzatore (a pagina 637)

Analisi della causa principale

Utilizzando Visualizer con Visualizzatore CMDBf, è possibile eseguire un'analisi della causa principale.

Per eseguire un'analisi della causa principale

1. In Visualizer, individuare un elemento della configurazione Servizio in una particolare condizione di problema (ad esempio lento o non disponibile).
2. Fare clic con ilo pulsante destro del mouse sull'elemento della configurazione e scegliere Elemento della configurazione con stato attivo.
3. Selezionare un filtro Causa principale utilizzando i seguenti criteri:
   - Tipo di classe: n/d
   - Relazione da fornitore a dipendente: tutte le relazioni da visualizzare per l'analisi della causa principale.
4. Fare clic su Visualizza.

   Nel grafico vengono visualizzati tutti gli elementi della configurazione correlati all'elemento della configurazione con stato attivo specificato nei filtri. Tutti i percorsi tra elementi della configurazione includono elementi della configurazione intermedi rispetto al livello predefinito.
5. Accedere agli elementi della configurazione e ispezionarli per incidenti, problemi o cambiamenti recenti che potrebbero essere la causa principale della condizione dell'elemento della configurazione con stato attivo.
6. Avviare CA CMDB in contesto per un determinato elemento della configurazione.
7. Fare clic su Visualizzatore CMDBf.

   Viene mostrata la visualizzazione federata con l'elenco dei fornitori MDR per l'elemento della configurazione.
8. Fare clic su Recupera per ottenere gli attributi MDR più recenti.

   Gli attributi MDR vengono aggiornati.

Amministrazione del visualizzatore

Nell'interfaccia di amministrazione del visualizzatore è possibile modificare le impostazioni di CMDB Visualizer. Queste funzioni sono disponibili solo per i ruoli con privilegi di amministratore.

Le schede seguenti vengono disabilitate sul Visualizer in esecuzione sui server secondari. Queste schede vengono abilitate su tutti gli altri server di CA SDM:

Scheda Configurazione visualizzatore

Consente di impostare le informazioni di visualizzazione del server e degli elementi della configurazione.

Scheda Stile di relazione

Consente di definire le caratteristiche grafiche della relazione.

Scheda Stato elemento della configurazione

Consente di definire le caratteristiche grafiche dell'elemento della configurazione.

Scheda Filtri

Consente di creare, modificare ed eliminare i filtri per l'analisi degli elementi della configurazione.

Scheda Configurazione icone

Mappa una famiglia di elementi della configurazione alla rispettiva immagine di icona se CMDB Visualizer è stato aggiornato da r11.2 a Versione 12.9.

Nota: per ulteriori informazioni sulle definizioni del visualizzatore, consultare la Guida in linea di CMDB Visualizer.

Aggiunta di un asset rilevato

È possibile modificare asset non posseduti in Gestione database (MDB) in elementi della configurazione posseduti.

Per aggiungere un asset rilevato

1. Fare clic sul pulsante Asseti rilevati della pagina Elenco dell'elemento della configurazione.

   Viene visualizzata la pagina Ricerca asset rilevati.

2. Fare clic su Cerca per visualizzare l'elenco Asset rilevati.
3. Selezionare dall'elenco l'asset che si desidera aggiungere come elemento della configurazione, quindi fare clic sull'asset con il pulsante destro del mouse e selezionare Crea nuovo elemento della configurazione dal menu di scelta rapida visualizzato.

   Viene visualizzata la pagina Crea nuovo elemento della configurazione che contiene informazioni sull'elemento in alcuni campi.

4. Compilare gli eventuali campi rimanenti relativi al nuovo elemento della configurazione, quindi fare clic su Continua.

   Nota: per creare un elemento della configurazione sono obbligatori solo i valori dei campi Nome e Classe.

5. Immettere i dati nei campi appropriati come richiesto nella scheda Attributi.

   La famiglia della classe selezionata per l'elemento della configurazione determina gli attributi visualizzati nella scheda. Le informazioni immesse nella scheda sono determinate dai processi di business e dalle informazioni che si desidera archiviare e visualizzare per un elemento della configurazione.

6. Fare clic su Salva.

   L'asset rilevato viene aggiunto.

Flag di asset ed elementi della configurazione

Due flag di attributo possono categorizzare ulteriormente il tipo di elemento della configurazione/asset per consentire di applicare filtri e controllare le entità visibili in CA SDM o in altri prodotti come CA APM.

I parametri sono i seguenti:

Elemento della configurazione? (SÌ/NO)

Identifica gli elementi della configurazione.

Asset? (SÌ/NO)

Identifica gli asset.

Per impostazione predefinita, un elemento della configurazione creato da CA CMDB viene contrassegnato come elemento della configurazione e non come asset. Se necessario, è possibile ignorare questa impostazione. Un elemento della configurazione può essere anche un asset. CA CMDB nn consente la modifica del flag Asset una volta impostato su Sì. Il flag Asset viene in genere impostato su Sì quando è stato creato un asset da CA APM.

Questi flag sono visualizzati in tutti i moduli dei dettagli degli elementi della configurazione e nello strumento di ricerca di elementi della configurazione. È possibile aggiornare il valore di questi flag nel modulo Dettagli elemento della configurazione, in GRLoader e nei servizi Web CA CMDB. Anche la funzione Modifica in elenco supporta l'aggiornamento dei nuovi flag in più record.

Il nome di attributo oggetto per il flag Elemento della configurazione è **is_ci**. Il nome di attributo oggetto per il flag Asset è **is_asset**. Questi nomi sono attributi SREL che fanno riferimento a bool. I nomi di attributo possono essere utilizzati come tag XML per GRLoader. Ad esempio, per modificare il valore predefinito del flag Asset quando si crea un elemento della configurazione con GRLoader, aggiungere il seguente codice XML per definire il nuovo elemento della configurazione:

```
<is_asset>YES</is_asset>
```

Riconciliazione elementi della configurazione

La riconciliazione aiuta a garantire che gli aggiornamenti da più origini di dati che fanno riferimento allo stesso oggetto di business aggiornino un solo elemento della configurazione, anche se questi possiedono tipi diversi di informazioni sull'identificazione. *L'ambiguità* rappresenta la possibilità che un elemento della configurazione non sia univoco. Può avere infatti dei "duplicati" nel CMDB e le transazioni dell'elemento della configurazione possono includere più di un elemento della configurazione di destinazione possibile. Gli elementi della configurazione ambigui possono portare a un malfunzionamento di CMDB, che nega il valore di CMDB e potrebbe causare azioni di business inappropriate.

La riconciliazione automatica di un elemento della configurazione è un vantaggio chiave di <CMBD>, che consente di risparmiare tempo rispetto alla manutenzione manuale dei dati. Il processo di riconciliazione di elementi della configurazione utilizza svariati attributi specifici dell'identificazione. Tuttavia, la riconciliazione automatica potrebbe generare:

- Falsi risultati positivi

  Vengono aggiornati elementi della configurazione esistenti invece di crearli.

- Falsi risultati negativi

  Nuovi elementi della configurazione vengono creati invece di aggiornare un elemento della configurazione esistente. L'insieme di elementi della configurazione con attributi di identificazione simili sono ambigui in quanto somigliano allo stesso oggetto di business reale con attributi di identificazione simili.

CA Service Desk Manager supporta i seguenti approcci di riconciliazione:

Riconciliazione basata su MDR (passiva)

Permettere a CMDB di riconciliare dati ambigui secondo il processo di riconciliazione basata su MDR.

Identificare e risolvere elementi della configurazione ambigui (reattiva)

Identificare e risolvere elementi della configurazione mediante l'identificazione e la gestione di elementi della configurazione esistenei in CMDB.

Rivedere e modificare dati in entrata utilizzando un'area di lavoro di transazione (proattiva)

Rivedere e modificare dati in entrata prima del caricamento in CMDB utilizzando un'area di lavoro della transazione (TWA).

Ulteriori informazioni:

Riconciliazione basata su MDR (a pagina 641)
Identificazione e risoluzione degli elementi della configurazione ambigui (a pagina 643)
Revisione e modifica di dati in entrata utilizzando l'area di lavoro della transazione (TWA) (a pagina 657)

Riconciliazione basata su MDR

La *riconciliazione basata su MDR* viene effettuata in MDR (Management Data Repository) per ridurre ulteriori occorrenze di vari elementi della configurazione nell'MDB che si riferisce allo stesso oggetto nel mondo fisico.

La riconciliazione basata su MDR considera MDR come una fonte sicura che utilizza sempre lo stesso ID asset federato quando comunica informazioni relative a un singolo elemento della configurazione. Tutti gli aggiornamenti da uno specifico MDR a uno specifico ID asset federato aggiornano sempre lo stesso elemento della configurazione, anche quando gli attributi identificativi vengono modificati.

La riconciliazione basata su MDR, la gestione della riconciliazione e l'area di lavoro transazione descritte in queste sezioni consentono di controllare il processo di riconciliazione. Tuttavia, per utilizzare correttamente la gestione della riconciliazione e l'area di lavoro transazione (TWA), è necessario capire come CA SDM usa gli attributi di riconciliazione.

Importante: se si reinstalla e reinizializza un fornitore di dati esterni (come CA Cohesion ACM), è necessario disattivare e riattivare la definizione dell'MDR nel CMDB. Se l'MDR riutilizza gli ID asset federati, è possibile che si verifichi una sovrapposizione accidentale degli elementi di configurazione.

Ulteriori informazioni:

Corrispondenza della riconciliazione di MDR e degli elementi della configurazione (a pagina 642)
Identificazione degli elementi della configurazione dalla riconciliazione MDR (a pagina 642)

Corrispondenza della riconciliazione di MDR e degli elementi della configurazione

La riconciliazione basata su MDR utilizza il seguente processo per identificare gli elementi della configurazione corrispondenti appropriati:

1. Se una transazione specifica un ID, l'elemento della configurazione viene identificato e la riconciliazione viene completata.
2. Se la transazione non specifica un ID, CA SDM esegue un controllo per verificare che gli attributi di identificazione federati siano specificati e corrispondano a un elemento della configurazione. Qualora corrispondano, viene eseguita la riconciliazione tra la transazione e l'elemento della configurazione corrispondente.
3. Se una transazione non specifica un ID o gli attributi di identificazione federati, la transazione dell'elemento della configurazione utilizza gli attributi di identificazione (a pagina 642) come specificato nella sezione seguente.

Identificazione degli elementi della configurazione dalla riconciliazione MDR

La riconciliazione basata su MDR utilizzare la seguente precedenza per identificare un elemento della configurazione:

1. ID (se una transazione specifica un ID, la riconciliazione è corretta)
2. Attributi di identificazione federati
   - ID asset federato
   - Nome MDR
   - Classe MDR
3. Attributi identificativi elemento della configurazione
   - Titolare (se è installata la funzionalità di multi-tenancy)
   - Nome
   - Numero di serie
   - Indirizzo MAC
   - Nome del sistema
   - ID asset alternativo
   - Nome DNS

Identificazione e risoluzione degli elementi della configurazione ambigui

Si consiglia di gestire le ambiguità degli elementi della configurazione caso per caso. In ogni caso, l'amministratore della configurazione deve rilevare la presenza di ambiguità e stabilire qual è l'approccio ottimale. CA SDM adotta un approccio flessibile per identificare e gestire eventuali elementi della configurazione duplicati già presenti in CMDB.

L'*indice di ambiguità* è una misura operativa della potenziale non unicità di un elemento della configurazione basata sugli attributi che lo identificano. Tale indice può misurare la probabilità che esistano elementi della configurazione "duplicati" nel CMDB o che una transazione possa avere più destinazioni di elementi della configurazione.

Importante. Se si eliminano manualmente gli elementi della configurazione con query del database, possono verificarsi degli errori per gli indici di ambiguità degli elementi della configurazione. Per evitare questi errori, eseguire l'utilità di cmdb_update_ambiguity e impostare il parametro -full su 1. Questo parametro consente di ricevere indici di ambiguità accurati durante l'esecuzione di cmdb_update_ambiguity.bat o dello script shell.

Utilizzare il processo indicato di seguito per identificare e risolvere elementi della configurazione ambigui:

1. Identificare elementi della configurazione ambigui.
   - Calcolare l'indice di ambiguità per tutti gli elementi della configurazione
   - Rivedere l'elenco degli elementi della configurazione ambigui dal contatore
2. Determinare se gli attributi di identificazione di ciascun elemento della configurazione sono validi.
3. Risolvere gli elementi della configurazione ambigui con una delle seguenti azioni:
   - Modificare gli attributi di identificazione
   - Escludere un elemento della configurazione dalla gestione delle ambiguità
   - Rifiutare l'aggiornamento di un elemento della configurazione disattivando l'elemento della configurazione
   - Sostituire un elemento della configurazione

Ulteriori informazioni:

Esempio di ambiguità degli elementi della configurazione (a pagina 644)
Modalità per l'identificazione degli elementi della configurazione ambigui e per la verifica dei loro attributi di identificazione (a pagina 645)
Modalità per la risoluzione degli elementi della configurazione ambigui (a pagina 653)

Esempio di ambiguità degli elementi della configurazione

I dati di quattro diverse fonti di dati vengono caricati in CMDB. Ciascuna fonte di dati utilizza il proprio sottoinsieme di caratteristiche di identificazione. A causa di questa incoerenza, è possibile che in CMDB siano presenti più elementi della configurazione di quelli desiderati.

Di seguito, sono riportati alcuni esempi di ambiguità degli elementi della configurazione:

Esempio: elementi della configurazione ambigui

I quattro elementi della configurazione indicati di seguito risiedono in CMDB:

- Nome (Server1) Nome DNS (dns1) Numero di serie (serial1)
- Nome (Server1) Nome DNS (dns1)
- Nome (Server2) Nome DNS (dns1) Numero di serie (serial1)
- Nome (Server3) Indirizzo MAC (mac1)

Poiché condividono le caratteristiche di identificazione, le due istanze di Server1 e Server2 sono ambigue l'una rispetto all'altra. L'istanza Server3 non è ambigua.

Ciascun elemento della configurazione è associato a un indice di ambiguità. L'indice di ambiguità corrisponde approssimativamente al numero di elementi della configurazione che corrispondono a uno qualsiasi degli attributi di identificazione. Più alto è l'indice e più elevato è il numero degli elementi della configurazione che corrispondono agli identificatori e maggiore è la probabilità che i dati degli elementi della configurazione siano stati inseriti in modo incoerente e che siano stati creati elementi della configurazione errati aggiuntivi errati. Gli elementi della configurazione con un indice di ambiguità pari a zero sono univoci in tutti gli identificatori e quindi non ambigui.

L'indice di ambiguità di ciascuno degli elementi della configurazione precedenti è:

- Prima istanza di Server1: conteggio degli elementi della configurazione che corrispondono a nome + nomedns + numero di serie = 1+2+ 1=4
- Seconda istanza di Server1: conteggio degli elementi della configurazione che corrispondono a nome + nomedns = 1+2 = 3
- Server2: conteggio degli altri elementi della configurazione che corrispondono a nome + nomedns + numero di serie = 0 +2+1 = 3
- Server3: conteggio degli altri elementi della configurazione che corrispondono a nome + indirizzo mac = 0+0 = 0

Ulteriori informazioni:

Modalità di calcolo dell'indice di ambiguità (a pagina 646)
Visualizzazione degli elementi della configurazione ambigui dalla scheda Amministrazione (a pagina 651)
Visualizzazione degli elementi della configurazione ambigui dal contatore (a pagina 652)

Modalità per l'identificazione degli elementi della configurazione ambigui e per la verifica dei loro attributi di identificazione

È necessario analizzare qualsiasi elemento della configurazione con un indice di ambiguità diverso da zero per determinare se è univoco o se è stato creato inavvertitamente a causa di una riconciliazione errata. Gli elementi della configurazione non sono di per se ambigui, ma possono esserlo nei confronti di altri elementi della configurazione. Un sistema può avere molti insiemi di elementi della configurazione ambigui e ciascun insieme può contenere elementi della configurazione con valori comuni per gli attributi di identificazione.

Quando si ricerca l'ambiguità di un elemento della configurazione, si ricerca anche l'ambiguità degli altri elementi della configurazione nello stesso insieme. Quando si risolve l'ambiguità di un elemento della configurazione singolo, si riduce o si elimina l'ambiguità degli altri elementi della configurazione nello stesso insieme.

CA SDM fornisce strumenti per la gestione della riconciliazione che permettono di ricercare gli elementi della configurazione ambigui e l'insieme di elementi della configurazione di cui fa parte. È possibile ricercare la causa sottostante dell'ambiguità e risolverla.

Per gestire un'ambiguità, effettuare le seguenti operazioni:

1. Calcolare l'indice di ambiguità per tutti gli elementi della configurazione.
2. Usare il contatore per visualizzare l'elenco degli elementi della configurazione ambigui. Il contatore elenca tutti gli elementi della configurazione ambigui, in ordine decrescente di ambiguità.
3. Partendo dall'elemento della configurazione con il livello di ambiguità più alto nel contatore:
    a. Ispezionare tutti gli elementi della configurazione nel suo insieme di ambiguità. La scheda Riconciliazione nel modulo Dettagli elemento della configurazione di un elemento della riconfigurazione singolo elenca tutti gli altri elementi della configurazione presenti nell'insieme di ambiguità.
    b. Determinare se tutti gli elementi della configurazione nell'insieme sono legittimi o se si è verificato un errore durante la riconciliazione. Rivedere gli attributi di identificazione e determinare se gli elementi della configurazione nell'insieme sono stati creati correttamente oppure sono stati creati a causa di una corrispondenza falsa negativa della riconciliazione.

4. Determinare quali elementi della configurazione nell'insieme sono falsi negativi, se applicabile.

   Dopo aver verificato che si è verificata una corrispondenza falsa negativa e che sono stati creati elementi della configurazione aggiuntivi, determinare quale elemento della configurazione è quello valido e quali elementi della configurazione sono stati creati in modo errato. Considerare fattori quali gli attributi di identificazione e altri attributi come la data dell'ultimo aggiornamento, i problemi correlati, le questioni e altri aspetti dell'elemento della configurazione.

Modalità di calcolo dell'indice di ambiguità

Prima di iniziare a gestire l'ambiguità, è necessario aggiornare l'indice di ambiguità per gli elementi della configurazione e delle transazioni degli elementi della configurazione esistenti. Per aggiornare l'indice di ambiguità per gli elementi della configurazione e le transazioni degli elementi della configurazione, è sufficiente eseguire il comando cmdb_update_ambiguity.

Importante È necessario eseguire cmdb_update_ambiguity almeno una volta per misurare l'ambiguità degli elementi della configurazione o delle transazioni degli elementi della configurazione. Se non si esegue il comando, tutti gli indici di ambiguità sono pari a 0 (zero), che corrisponde a nessuna ambiguità.

È possibile eseguire l'utilità prima e durante la gestione delle ambiguità. È possibile pianificare l'esecuzione regolare dell'utilità in modo che gli indici di ambiguità riflettano lo stato corrente del sistema.

Per utilizzare l'indice di ambiguità

1. Determinare i parametri necessari per l'esecuzione dell'utilità.
2. Eseguire l'utilità.
3. Avviare il client Web CA SDM e passare a Elemento della configurazione ambiguo o alla pagina degli elenchi delle transazioni degli elementi della configurazione ambigui per gestire l'ambiguità.

Ulteriori informazioni:

Identificazione e risoluzione degli elementi della configurazione ambigui (a pagina 643)

Comando cmdb_update_ambiguity

È possibile calcolare indici di ambiguità degli elementi della configurazione e delle transazioni degli elementi della configurazione utilizzando una sintassi di comando simile a quella riportata di seguito:

```
cmdb_update_ambiguity [parametri] –m { ci | twa | all }
```

Per i parametri di comando, vedere Parametri di cmdb_update_ambiguity (a pagina 649).

Per impostazione predefinita, la scansione degli elementi della configurazione è eseguita dalla data dell'ultima scansione. Se si specifica "-full 1", viene eseguita una scansione completa.

Esempio: calcolo dell'ambiguità degli elementi della configurazione in un database Microsoft SQL Server

Il seguente comando calcola l'indice di ambiguità per tutti gli elementi della configurazione e le transazioni esistenti nell'area di lavoro della transazione:

```
cmdb_update_ambiguity –m all –d MSSQL –u servicedesk –p dbpassword -s dbserver1
```

Esempio: calcolo dell'ambiguità di elementi della configurazione in database Oracle

Il seguente comando calcola l'indice di ambiguità per tutti gli elementi della configurazione e specifica le informazioni relative al database.

```
Comando cmdb_update_ambiguity –m ci –d Oracle –u mdbadmin –p dbpassword -s server1
-port 1521 –SID orcl
```

Modalità di utilizzo di un file di configurazione

In un file di configurazione è possibile specificare più parametri cmdb_update_ambiguity. È possibile utilizzare il file di configurazione per proteggere impostazioni di parametri in un formato crittografato mediante strumenti del sistema operativo. Le parole chiave valide e le opzioni della riga di comando corrispondenti sono elencate nella tabella dei parametri.

Nota: se si specifica un parametro sia nella riga di comando che in un file di configurazione, il valore della riga di comando prevale su quello nel file di configurazione.

Esempio: utilizzo di un file di configurazione per specificare i parametri per un database SQL Server

Il seguente comando esegue il file di configurazione ambiguity_mssql.cfg.

```
cmdb_update_ambiguity –m all -c ambiguity_mssql.cfg
```

Formato del file di configurazione

Le opzioni del file di configurazione sono specificate come *parola chiave*=*valore*. In Windows, il separatore di directory può essere una doppia barra rovesciata (\\) oppure una barra singola (/). Il nome del percorso deve essere racchiuso tra virgolette ("").

Le parole chiave valide e le opzioni della riga di comando corrispondenti sono elencate nella tabella dei parametri.

Note: un marcatore hash (#) nella colonna 1 indica l'inizio di una riga di commento.

Esempio: impostazioni di configurazione di Microsoft SQL Server

```
#File di configurazione di esempio per Microsoft SQL Server
DBType=MSSQL
DBUser=servicedesk
DBPassword=dbpassword
DBHost=dbserver1
LogLocation=C:\\Programmi\\CA\\Service Desk Manager\\log
LogLevel=ERROR
SchemaName=dbo
```

Esempio: impostazioni di configurazione Oracle

```
#File di configurazione di esempio per Oracle
DBType=Oracle
DBUser=mdbadmin
DBPassword=dbpassword
DBHost=dbserver1
LogLocation=/tmp/ambiguity/log
LogLevel=INFO
DBPort=1521
DBSID=orcl
SchemaName=mdbadmin
```

Parametri cmdb_update_ambiguity

È possibile specificare parametri nella riga di comando oppure in un file configurabile (alcuni parametri sono solo per la riga di comando). Nella riga di comando utilizzare le virgolette ("") per racchiudere eventuali nomi di percorso con spazi; nel file di configurazione non utilizzare virgolette. Se si specificano parametri sia nella riga di comando che nel file di configurazione, il valore della riga di comando prevale sul valore del file di configurazione.

Il comando cmdb_update_ambiguity è caratterizzato dai seguenti parametri:

Opzione	Password file di configurazione	Valori	Note
-m	(nessuno)	twa, ci, all	(Obbligatorio) Solo per riga di comando twa = calcola ambiguità solo su area di lavoro transazione. ci = calcola ambiguità solo per elementi della configurazione. all = calcola ambiguità per elementi della configurazione e area di lavoro transazione.
-d	"dbType"	MSSQL o Oracle	(Richiesto. Solo Windows). Tipo di database. In Linux/UNIX, è supportato solo Oracle e questa opzione non è necessaria.
-u	DBUser	<nome utente database>	(Richiesto) Nome utente del database. Un nome utente con spazi deve essere racchiuso tra virgolette (ad esempio: -u "sys as sysdba"). I punti di domanda non sono richiesti nel file di configurazione.
-p	DBPassword	<password database>	(Richiesto) Password per l'utente database. Una password con spazi deve essere racchiusa tra virgolette (ad esempio: -p "codice segreto"). I punti di domanda non sono richiesti nel file di configurazione.
-c	(nessuno)	<file di configurazione>	(Facoltativo) Solo per riga di comando Nome completo del percorso del file di configurazione. Deve essere racchiuso tra virgolette se contiene spazi.

-log	LogLocation	<directory del file di registro>	(Facoltativo). Directory del file di registro Il percorso predefinito è la directory NX_ROOT\log .
-level	LogLevel	INFO, ERROR, DEBUG	(Facoltativo). Livello di dettaglio per la scrittura nel file di registro. Il valore predefinito è ERROR.
-s	DBHost	<nome server>	(Richiesto) Nome host del server database. Per utilizzare un'istanza denominata Microsoft SQL Server, specificare *server**istanza* nella riga di comando o *server**istanza* nel file della configurazione.
-CI	Elemento della configurazione	<uuid dell'elemento della configurazione>	(Facoltativo). Calcola l'ambiguità dell'elemento della configurazione specificato e di tutti gli elementi della configurazione che sono ambigui rispetto ad esso.
-full	(nessuno)	0,1	(Facoltativo) Solo per riga di comando Ottimizza le prestazioni della scansione prendendo in esame solo gli elementi della configurazione aggiornati dopo l'ultima esecuzione dell'utilità. Se si imposta questa opzione su 1, viene eseguita una scansione completa forzata di tutti gli elementi di configurazione durante il calcolo dell'indice di ambiguità. L'impostazione predefinita è 0. Questo parametro non si applica al calcolo dell'ambiguità delle transazioni. L'utilità valuta sempre tutte le transazioni in TWA.
-port	DBPort	<numero porta>	(Richiesto. Solo Oracle) Numero porta Oracle
-SID	DBSID	<nome SID>	(Richiesto. Solo Oracle) Nome SID Oracle
-h	(nessuno)		(Facoltativo). Stampa il messaggio di utilizzo di aiuto.
-schema	SchemaName	<nome schema database>	(Facoltativo). L'impostazione predefinita è mdbadmin per Oracle o dbo per Microsoft SQL Server.

Ulteriori informazioni:

Comando cmdb_update_ambiguity (a pagina 647)

Visualizzazione degli elementi della configurazione ambigui dalla scheda Amministrazione

Dopo l'esecuzione dell'utilità cmdb_update_ambiguity, è possibile visualizzare e gestire gli elementi della configurazione tramite la scheda Amministrazione.

Per visualizzare le transazioni degli elementi della configurazione ambigue, nella scheda Amministrazione selezionare CA CMDB, Gestione riconciliazione Elementi della configurazione ambigui.

La pagina Elenco Elementi della configurazione ambigui visualizza l'elenco degli elementi della configurazione con un indice superiore a 0 (zero).

Nota: quando si seleziona Cancella filtro nella pagina Elenco Elementi della configurazione ambigui, il campo Altri argomenti di ricerca non viene cancellato (ambiguità > 0).

Ulteriori informazioni:

Visualizzazione degli elementi della configurazione ambigui dalla scheda Amministrazione (a pagina 651)

Visualizzazione degli elementi della configurazione ambigui dal contatore

Dopo l'esecuzione dell'utilità cmdb_update_ambiguity, è possibile visualizzare e gestire gli elementi della configurazione tramite il contatore.

Per visualizzare le transazioni degli elementi della configurazione ambigue dal contatore:

1. Dall'interno del contatore CA SDM, espandere la cartella CMDB.
2. Selezionare Gestione riconciliazione, Elementi della configurazione ambigui, quindi fare clic su una delle seguenti opzioni:
   - Tutti
   - Aggiornate all'ultimo giorno
   - Aggiornate all'ultima settimana
   - Aggiornate all'ultimo mese

   Viene visualizzato l'elenco degli elementi della configurazione ambigui con un indice superiore a 0 (zero).

   Nota: quando si seleziona Cancella filtro nella pagina Elenco Elementi della configurazione ambigui, il campo Altri argomenti di ricerca non viene cancellato (ambiguità > 0).

Ulteriori informazioni:

Identificazione e risoluzione degli elementi della configurazione ambigui (a pagina 643)

Modalità per la risoluzione degli elementi della configurazione ambigui

Dopo aver identificato gli elementi della configurazione ambigui e aver stabilito se i loro attributi di identificazione sono validi, è necessario risolvere l'ambiguità tra gli elementi della configurazione nell'insieme di ambiguità effettuando una o più delle operazioni descritte di seguito.

Modificare gli attributi di identificazione

Se si determina che gli attributi di identificazione non sono completi o validi, impostare gli attributi di identificazione dell'elemento della configurazione in modo che l'elemento della configurazione risulti univoco utilizzando l'interfaccia Web, GRLoader o CMDBf.

Nota: quando l'MDR aggiorna l'elemento della configurazione, può annullare le modifiche della riconciliazione effettuate manualmente.

Escludere un elemento della configurazione dalla gestione delle ambiguità

Se si determina che le caratteristiche di identificazione degli elementi della configurazione sono corretti e rappresentano un'ambiguità conosciuta e valida, è possibile rimuovere l'elemento della configurazione dagli elenchi di gestione delle ambiguità e dal calcolo delle ambiguità degli altri elementi della configurazione. Inoltre, è possibile contrassegnare l'elemento della configurazione come non ambigua, ovvero escludere l'ambiguità.

Rifiutare l'aggiornamento di un elemento della configurazione disattivando l'elemento della configurazione

Se si determina che gli attributi di identificazione di un elemento della configurazione sono errati e che gli aggiornamenti che utilizzano tali dati corrompono i dati, è possibile disattivare l'elemento della configurazione per impedire successivi aggiornamenti. L'utente o l'MDR che genera le informazioni riceve un errore e l'intera transizione viene rifiutata.

Sostituire un elemento della configurazione

Gli aggiornamenti a CMDB esulano talvolta dal controllo dell'amministratore ed è necessario che nel sistema siano presenti sia dati di identificazione non validi sia dati di attributi di non identificazione validi. I dati degli attributi della transizione in entrata possono essere reindirizzati in modo trasparente all'elemento della configurazione sostitutivo.

Nota: il reindirizzamento trasparente dei dati degli attributi da un elemento della configurazione a un altro può creare confusione perché i dati della transizione potrebbero non essere stati memorizzati nello stesso elemento della configurazione come invece indurrebbero a pensare gli attributi di identificazione della transazione. È consigliabile usare questo metodo con discrezione e solo se i metodi precedenti non possono essere usati.

Modalità di esclusione di elementi della configurazione dalla gestione dell'ambiguità

Talvolta è chiaro che, anche se un determinato elemento della configurazione ottiene un indice di ambiguità superiore a zero, deve essere lasciato invariato. Qualsiasi elemento della configurazione che abbia la casella di controllo Escludi ambiguità selezionata non è considerato parte dell'indice di ambiguità o delle funzionalità di gestione dell'ambiguità.

Esclusione dall'ambiguità per un elemento della configurazione

È possibile aggiornare l'opzione di esclusione dell'ambiguità per un elemento della configurazione dall'interfaccia Web.

Per escludere l'ambiguità per un elemento della configurazione

1. Selezionare dalla pagina Elenco elementi della configurazione ambigui l'elemento della configurazione che si desidera rimuovere dalla gestione dell'ambiguità.

   Viene visualizzata la pagina Dettagli elemento della configurazione.

2. Fare clic su Modifica.

   Viene visualizzata la pagina Aggiorna elemento della configurazione.

3. Selezionare la casella di controllo Escludi ambiguità dalla scheda Riconciliazione, quindi fare clic su Salva.

   L'elemento della configurazione viene escluso dal calcolo dell'indice di ambiguità e da altre funzionalità di gestione dell'ambiguità.

Modalità di esclusione dell'ambiguità con GRLoader

È possibile aggiornare l'opzione di esclusione dell'ambiguità per un elemento della configurazione utilizzando GRLoader per impostare il flag not_ambiguous per l'elemento della configurazione.

Di seguito sono elencati i possibili valori di not_ambiguous:

SÌ (1)

Rimuove l'elemento della configurazione dalla gestione dell'ambiguità. L'elemento della configurazione è identificato come univoco, indipendentemente dagli attributi identificativi di altri elementi della configurazione. L'indice di ambiguità dell'elemento della configurazione rimane zero.

NO (0) (predefinito)

L'elemento della configurazione è idoneo per la gestione dell'ambiguità. L'unicità degli attributi di identificazione dell'elemento della configurazione determina l'indice di ambiguità di questo elemento della configurazione. Gli attributi identificativi dell'elemento della configurazione vengono considerati quando viene valutato l'indice di ambiguità di altri elementi della configurazione.

Nota: per ulteriori informazioni su GRLoader, consultare la *Guida di riferimento tecnico di CA CMDB*.

Modalità di rifiuto di aggiornamenti

Quando un elemento della configurazione è contrassegnato come Non attivo, non è più possibile aggiornarlo. Se si desidera che CA CMDB rifiuti i dati di un determinato elemento della configurazione (sia in base al nome, al numero di serie, all'indirizzo MAC e così via) e si desidera l'MDR sia a conoscenza del rifiuto, impostare l'elemento della configurazione su Non attivo.

In questo modo è possibile rifiutare immediatamente dati problematici e intervenire anche sull'origine, dove l'MDR può correggere l'input rifiutato.

Per impostare un elemento della configurazione su Non attivo nell'interfaccia Web, modificare l'elemento della configurazione, impostarlo su Non attivo e fare clic su Salva. È possibile impostare un elemento della configurazione su Non attivo utilizzando GRLoader oppure i servizi Web di CMDBf. È possibile anche riattivare gli elementi della configurazione disattivati.

Sostituzione di elementi della configurazione ambigui

È possibile sostituire un elemento della configurazione ambiguo per reindirizzare i dati a un elemento della configurazione di destinazione specifico. Gli amministratori possono visualizzare elementi della configurazione sostituiti, che sono non attivi, e tutti gli aggiornamenti apportati ad essi dall'interfaccia Web verranno ignorati.

Nota: gli aggiornamenti inviati a elementi della configurazione sostituiti da GRLoader o da servizi Web CMDBf sono reindirizzati all'elemento della configurazione sostitutivo. Tuttavia, gli aggiornamenti relativi agli attributi di identificazione vengono ignorati.

Per sostituire un elemento della configurazione ambiguo:

1. Selezionare l'elemento della configurazione da impostare come attivo (elemento della configurazione sostitutivo) nella pagina Elenco Elementi della configurazione ambigui.

   Viene visualizzata la pagina Dettagli elemento della configurazione.

2. Fare clic su Modifica.

   Viene visualizzata la pagina Aggiorna elemento della configurazione.

3. Fare clic sulla scheda Riconciliazione.

   Vengono visualizzati tutti gli elementi della configurazione ambigui all'interno dell'elemento della configurazione attivo.

   Determinare gli elementi della configurazione che si desidera sostituire con l'elemento della configurazione attivo. Ispezionare ciascun elemento della configurazione presente nell'elenco facendo clic su ciascun elemento della configurazione nella pagina Dettagli elemento della configurazione.

4. Selezionare uno o più elementi della configurazione ambigui da sostituire con l'elemento della configurazione attivo e fare clic su Sostituisci.

   L'elemento della configurazione attivo sostituisce gli elementi della configurazione selezionati.

Visualizzazione dalla scheda Amministrazione degli elementi della configurazione sostituiti

È possibile visualizzare gli elementi della configurazione sostituiti tramite la scheda Amministrazione.

Per visualizzare gli elementi della configurazione dalla scheda Amministrazione, nella scheda Amministrazione selezionare CA CMDB, Gestione riconciliazione, Elementi della configurazione sostituiti.

Viene visualizzato l'elenco degli elementi della configurazione sostituiti

Visualizzazione dal contatore degli elementi della configurazione sostituiti

È possibile visualizzare gli elementi della configurazione sostituiti tramite il contatore.

Per visualizzare gli elementi della configurazione sostituiti utilizzando il contatore:

1. Dall'interno del contatore CA SDM, espandere la cartella CMDB.
2. Espandere la cartella Gestione riconciliazione
3. Fare clic sul nodo dell'elemento della configurazione sostituito.

   Viene visualizzato l'elenco degli elementi della configurazione sostituiti

Revisione e modifica di dati in entrata utilizzando l'area di lavoro della transazione (TWA)

Prima dell'esecuzione è possibile verificare le transazioni per elementi della configurazione e di relazione copiando i dati nell'area a gestione temporanea dell'area di lavoro della transazione (TWA). Una volta nell'area a gestione temporanea, è possibile manipolare gli elementi della configurazione e le relazioni utilizzando l'interfaccia Web oppure l'SQL nativo.

È anche possibile convalidare le transazioni dell'elemento della configurazione per impedire che ne vengano creati di nuovi quando sarebbe necessario aggiornare un elemento della configurazione esistente. Con questo approccio è possibile visualizzare ogni transazione e gli elementi della configurazione potenziali che può aggiornare in modo da poter riconciliare manualmente la transazione con l'elemento della configurazione di destinazione. Allo stesso modo, è possibile convalidare transazioni di relazione per indicare gli elementi della configurazione corretti.

L'*indice di ambiguità* è una misura operativa della potenziale non unicità di un elemento della configurazione basata sugli attributi che lo identificano. Tale indice può misurare la probabilità che esistano elementi della configurazione "duplicati" nel CMDB o che una transazione possa avere più destinazioni di elementi della configurazione.

Rivedere e modificare elementi della configurazione ambigue utilizzando il processo seguente:

1. Identificare transazioni di elementi della configurazione ambigui.
   - Calcolare l'indice di ambiguità per tutte le transazioni dell'elemento della configurazione
   - Rivedere l'elenco degli elementi della configurazione ambigui dal contatore
2. Determinare se gli attributi di identificazione per ciascun elemento della configurazione possono essere riconciliati con l'elemento della configurazione richiesto.
3. Risolvere gli elementi della configurazione ambigui effettuando una delle azioni seguenti:
   - Modificare gli attributi di identificazione
   - Specificare l'elemento della configurazione di destinazione

Ulteriori informazioni:

Esempio di ambiguità di una transazione degli elementi della configurazione (a pagina 659)
Modalità per l'identificazione di una transazione di elementi della configurazione ambigui (a pagina 661)
Modalità per la risoluzione delle transazioni degli elementi della configurazione ambigue (a pagina 662)
Area di lavoro transazione (a pagina 664)
Compilazione dell'area di lavoro transazione (TWA) (a pagina 666)
Modalità di utilizzo dell'interfaccia Web per aggiornare i dati nell'area di lavoro transazione (TWA) (a pagina 678)
Gestione di transazioni con installazione di appoggio (a pagina 663)
Modalità di caricamento delle transazioni in CMDB (a pagina 682)
Riconciliazione manuale (a pagina 680)
Amministrazione dell'area di lavoro transazione (TWA) (a pagina 684)

Esempio di ambiguità di una transazione degli elementi della configurazione

I dati delle transazioni provenienti da fonti diverse vengono caricati in CA CMDB. Ciascuna fonte dati utilizza il proprio sottoinsieme di caratteristiche di identificazione e potrebbe quindi non essere possibile identificare completamente gli elementi della configurazione di destinazione per le transazioni. A causa di questa incoerenza, è possibile che in CA CMDB ci siano più transazioni degli elementi della configurazione validi.

Di seguito viene riportato un esempio di ambiguità di una transazione degli elementi della configurazione:

Esempio: transazioni degli elementi della configurazione ambigui

Le seguenti transazioni degli elementi della configurazione risiedono in TWA:

- Nome (Server1) Nome DNS (dns1), Numero di serie (serial1)

I seguenti elementi della configurazione risiedono in CA CMDB:

- Nome (Server2) Nome DNS (dns1)
- Nome (Server3) Nome DNS (dns1), Numero di serie (serial1)
- Nome (Server4) Indirizzo MAC (mac1), Numero di serie (serial1)

Poiché condividono le caratteristiche di identificazione, la transazione Server1 è ambigua rispetto alle transazioni Server2, Server3 e Server4 in CA CMDB.

Ciascuna transazione degli elementi della configurazione è associata a un indice di ambiguità. L'indice di ambiguità corrisponde approssimativamente al numero di elementi della configurazione esistenti che corrispondono a uno qualsiasi degli attributi di identificazione, meno uno, specificati nella transazione degli elementi della configurazione. Più alto è l'indice e maggiore è il numero degli altri elementi della configurazione che corrispondono agli identificatori della transazione e conseguentemente maggiore è la probabilità che i dati degli elementi della configurazione inseriti siano incoerenti e che siano stati creati elementi della configurazione aggiuntivi errati. Le transazioni degli elementi della configurazione con un indice di ambiguità pari a zero hanno attributi di identificazione univoci in tutti gli elementi della configurazione oppure hanno un elemento della configurazione di destinazione specificato e non quindi ambigue.

Esempio: calcolo dell'indice di ambiguità

Le seguenti transazioni degli elementi della configurazione risiedono in TWA:

- Nome (Server1) Nome DNS (dns1), Numero di serie (serial1)
- Nome (Server2) Nome DNS (dns1), Numero di serie (serial1)

I seguenti elementi della configurazione risiedono in CA CMDB:

- Nome (Server1) Nome DNS (dns1), Numero di serie (serial1)
- Nome (Server2) Nome DNS (dns1), Numero di serie (serial1), Indirizzo MAC (mac1)

L'ambiguità della prima transazione (Server1) è 0 perché corrisponde esattamente agli attributi di identificazione degli elementi della configurazione della transazione Server1. L'unico elemento della configurazione di destinazione possibile per questa transazione è l'elemento della configurazione di Server1.

La seconda transazione (Server2) è ambigua rispetto all'elemento della configurazione di Server1 e Server2.

L'indice di ambiguità di Server1 è costituito dai seguenti componenti:

- Numero di elementi della configurazione che corrispondono a Nome (Server2) = 1
- Numero di elementi della configurazione che corrispondono a Nome DNS (dns1) = 2
- Numero degli elementi della configurazione che corrispondono a Numero di serie (serial1) = 2

In base delle caratteristiche di identificazione degli elementi della configurazione condivise, l'indice di ambiguità della transazione Server2 è (1-1) + (2-1) + (2-1) = 2

Modalità per l'identificazione di una transazione di elementi della configurazione ambigui

È possibile rivedere e modificare transazioni che hanno elementi della configurazione di destinazione ambigui prima di caricare i dati delle transazioni. È inoltre possibile risolvere transazioni per elementi della configurazione che non hanno un elemento della configurazione di destinazione ma hanno attributi identificativi per uno o più elementi della configurazione. Questa fase della risoluzione verificare che l'elemento della configurazione appropriato venga aggiornato ed evita che vengano creati dati errati o non coerenti.

La scheda Riconciliazione nella pagina Dettagli elemento della configurazione elenca tutti gli elementi della configurazione che risultano ambigui rispetto alla transazione dell'elemento della configurazione attivo. Ispezionare tutti gli attributi dell'elemento della configurazione quali la data dell'ultimo aggiornamento, i problemi correlati, le Issue e gli altri aspetti dell'elemento della configurazione per identificare l'elemento della configurazione di destinazione che corrisponde a tale transazione.

Nota: per visualizzare l'ambiguità degli elementi della configurazione o delle transazioni degli elementi della configurazione, è necessario calcolare l'indice di ambiguità con l'utilità cmdb_update_ambiguity utility (a pagina 647).

Per ulteriori informazioni, consultare Revisione e modifica dei dati in entrata tramite TWA (Transaction Work Area) (a pagina 657).

Visualizzazione delle transazioni ambigue dalla scheda Amministrazione

È possibile visualizzare e gestire le transazioni ambigue dalla scheda Amministrazione.

Per visualizzare le transazioni ambigue, nella scheda Amministrazione selezionare CA CMDB, Gestione riconciliazione, Transazioni elemento della configurazione ambiguo.

Viene visualizzato l'elenco delle transazioni degli elementi della configurazione con un indice di ambiguità superiore a 0 (zero).

Nota: quando si seleziona Cancella filtro nella pagina Elenco Elementi della configurazione ambigui, il campo Altri argomenti di ricerca non viene cancellato (ambiguità > 0).

Visualizzazione delle transazioni ambigue dal contatore

È possibile visualizzare e gestire le transazioni ambigue dal contatore.

Per visualizzare le transazioni ambigue dal contatore:

1. Dall'interno del contatore CA SDM, espandere la cartella CMDB.
2. Selezionare Gestione riconciliazione, Transazioni elemento della configurazione ambiguo, quindi fare clic su una delle seguenti opzioni:
   - Tutti
   - Aggiornate all'ultimo giorno
   - Aggiornate all'ultima settimana
   - Aggiornate all'ultimo mese

   Viene visualizzato l'elenco delle transazioni degli elementi della configurazione con un indice di ambiguità superiore a 0 (zero).

   Nota: quando si seleziona Cancella filtro nella pagina Elenco Elementi della configurazione ambigui, il campo Altri argomenti di ricerca non viene cancellato (ambiguità > 0).

Modalità per la risoluzione delle transazioni degli elementi della configurazione ambigue

Dopo aver identificato le transazioni degli elementi della configurazione ambigue e stabilito se i loro attributi di identificazione o l'elemento della configurazione di destinazione sono validi, è possibile risolvere l'ambiguità tra le transazioni degli elementi della configurazione effettuando una delle operazioni descritte di seguito.

Modificare gli attributi di identificazione

Se si determina che gli attributi di identificazione non sono completi o validi, è possibile impostare gli elementi di identificazione dell'elemento della configurazione in modo che l'elemento della configurazione risulti univoco quando si utilizza l'interfaccia Web.

Impostazione dell'elemento della configurazione di destinazione

Se si determina che l'elemento della configurazione di destinazione non è impostato o valido, è possibile specificare un elemento della configurazione per una transazione ambigua in modo che i dati vengano reindirizzati a un elemento della configurazione di destinazione specifico indipendentemente dai valori degli attributi di identificazione specificati nella transazione.

Definizione di un elemento della configurazione di destinazione per una transizione dell'elemento della configurazione ambigua

È possibile specificare un elemento della configurazione per una transazione ambigua in modo che i dati vengano indirizzati a un elemento della configurazione di destinazione specifico, indipendentemente dai valori di identificazione specificati nella transazione.

Per specificare un elemento della configurazione di destinazione per una transazione dell'elemento della configurazione ambigua:

1. Selezionare una transazione dell'elemento della configurazione nella pagina Elenco Transazioni ambigue.

   Viene visualizzata la pagina dei dettagli della transizione dell'elemento della configurazione.

2. Fare clic su Modifica.

   Viene visualizzata la pagina Aggiorna elemento della configurazione.

3. Nella scheda Riconciliazione selezionare un elemento della configurazione dall'elenco per impostare l'elemento della configurazione come elemento della configurazione di destinazione per la transazione. Fare clic su Imposta destinazione, quindi fare clic su Salva.

   L'elemento della configurazione selezionato diventa quello di destinazione per la transazione.

Gestione di transazioni con installazione di appoggio

CA CMDB offre una struttura in cui è possibile archiviare dati prima di caricarli in CA CMDB. Questi dati con "installazione di appoggio" vengono archiviati come transazioni nell'area di lavoro transazione (TWA). Una transazione con installazione di appoggio rappresenta un'unità di lavoro che crea o aggiorna un elemento della configurazione o una relazione. L'area di lavoro transazione (TWA) può contenere molte transazioni per un dato elemento della configurazione o relazione.

È possibile catturare i dati caricati nel CMDB prima che tali dati vengano impegnati in modo da consentire le seguenti modifiche:

- È possibile pulire e adattare agli standard dati non standard.
- È possibile integrare dati incompleti. Ad esempio, i nomi degli elementi della configurazione che iniziano con "NY" possono avere l'ubicazione impostata su "New York".
- È possibile modificare dati che non corrispondono alle tabelle di ricerca esistenti (SREL).
- È possibile posticipare l'implementazione di transazioni.

- Riconciliare le transazioni agli elementi di configurazione esistenti nel CA CMDB prima di caricare i dati.
- È anche possibile convalidare le transazioni degli elementi di configurazione e di relazione per impedire la creazione di dati non validi o nuovi elementi di configurazione quando avrebbero dovuto essere aggiornati elementi della configurazione singoli o esistenti. Con questo approccio è possibile visualizzare ogni transazione e gli elementi della configurazione potenziali che può aggiornare in modo da poter riconciliare manualmente la transazione con l'elemento della configurazione di destinazione.

È possibile utilizzare l'area di lavoro transazione (TWA) per consentire la gestione proattiva del processo di riconciliazione. È possibile configurare GRLoader per caricare i dati nell'area di lavoro transazione (TWA), dove CA CMDB consente di modificare i dati della transazione per gestire le transazioni che possono creare aggiornamenti potenziali o fare riferimento all'elemento della configurazione errato.

Per ulteriori informazioni, consultare Revisione e modifica dei dati in entrata tramite TWA (Transaction Work Area) (a pagina 657).

Area di lavoro transazione

CA SDM fornisce l'area di lavoro transazione (TWA) per ispezionare e modificare dati dell'elemento della configurazione e della relazione prima di caricare i dati in CMDB.

Il processo dell'area di lavoro transazione funziona nel seguente modo:

1. Caricare i dati (a pagina 666)nell'area di lavoro transazione (TWA). Il contenuto può includere le transazioni dell'elemento della configurazione o le transazioni di relazione. Il processo di input non esegue il tentativo di riconciliare i record, bensì riempie semplicemente l'area di lavoro con i record dell'elemento della configurazione e delle transazioni di relazione in due modi:
   - GRLoader – Legge i dati XML e li archivia nell'area di lavoro transazione (TWA) utilizzando le opzioni -lttwa o -lttwar.
   - SQL nativo – I dati vengono inseriti nell'area di lavoro transazione (TWA) attraverso il processo SQL standard.
   - Creare una transazione dell'elemento della configurazione o una transazione di relazione utilizzando l'interfaccia Web.

2. (Opzionale) Riconciliare manualmente le transazioni agli elementi di configurazione esistenti nel CMDB prima di caricare i dati. È anche possibile simulare il caricamento dei dati (a pagina 671) per predeterminare se una serie di transazioni può creare nuovi elementi della configurazione (e pertanto creare nuove ambiguità per altri elementi della configurazione) o relazioni.

   Per ulteriori informazioni, consultare Revisione e modifica dei dati in entrata tramite TWA (Transaction Work Area) (a pagina 657).

3. Modificare i dati. È possibile modificare l'area di lavoro transazione (TWA) da una delle seguenti origini:

   Interfaccia utente di CA SDM

   L'interfaccia utente basata sul Web consente di visualizzare e modificare transazioni nell'area di lavoro transazione.

   SQL nativo

   Quando si eseguono numerose modifiche a più transazioni, i dati nell'area di lavoro transazione possono venire modificati dall'SQL nativo.

   Nota: le modifiche effettuate utilizzando SQL nativo possono eludere tutta la protezione di CA SDM.

4. GRLoader carica i dati dall'area di lavoro transazione (TWA) al CA CMDB utilizzando le opzioni -lftwa o -lftwai. Ogni fila dell'area di lavoro transazione vengono considerati come una transazione separata.

   1. Se si verifica un errore dopo l'avvio di GRLoader, il codice di errore viene immesso nella transazione per indicare che lo stato di quest'ultima è incompleto (per facilitare i tentativi successivi).
   2. Tutti i record vengono identificati come transazioni complete.

5. Rivedere i risultati della transazione e correggere eventuali errori utilizzando l'interfaccia Web. Ripetere i passaggi 3 e 4, se necessario.

   Note:

   - se sono state create famiglie o attributi personalizzati e si desidera che le rispettive colonne compaiano nell'area di lavoro, è necessario modificare l'area di lavoro per includervi le colonne personalizzate. Per ulteriori informazioni, vedere Estensione dell'oggetto TWA (a pagina 685).
   - Utilizzare la versione più recente di GRLoader per sfruttare l'area di lavoro transazione (TWA). Se si utilizza un prodotto che include una versione precedente di GRLoader, aggiornare GRLoader all'ultima versione.
   - Le modifiche apportate alle transazioni nell'area di lavoro transazione (TWA) non vengono monitorate.

Compilazione dell'area di lavoro transazione (TWA)

I dati di input possono provenire da un diverse origini:

- Prodotti CA quali CA Cohesion ACM, CA Wily CEM, CA Wily Introscope e CA Spectrum che consentono l'importazione mediante GRLoader
- MDR in grado di eseguire l'importazione dei dati mediante GRLoader
- Un altro CMDB
- Fogli di lavoro Microsoft Excel
- Tabelle di database
- Uno strumento ETL scelto da un vendor.

Per ulteriori informazioni, vedere Limitazioni del database (a pagina 688).

Modalità di caricamento dati nell'area di lavoro transazione (TWA) con GRLoader

Le seguenti opzioni di GRLoader supportano l'uso dell'area di lavoro transazione (TWA):

-lttwa

Carica dati XML nella TWA nello stato iniziale.

-lttwar

Carica dati XML nella TWA nello stato pronto.

-lftwa

Carica transazioni in the CMDB dall'area di lavoro transazione (TWA).

-lftwai

Carica transazioni in CMDB dalla TWA e disattiva transazioni riuscite.

È possibile caricare documenti di input XML di GRLoader in CMDB o nell'area di lavoro transazione (TWA) senza modifiche.

Il caricamento di dati nell'area di lavoro transazione può essere eseguito utilizzando dell'opzione –lttwa (carica in TWA) di GRLoader. Nel file di configurazione di GRLoader:

```
grloader.loadtotwa=yes
```

In modalità TWA, invece di creare direttamente gli elementi della configurazione e le relazioni, GRLoader inserisce le informazioni nelle tabelle dell'area di lavoro transazione. Al termine del caricamento nell'area di lavoro transazione, i dati possono essere modificati e verificati. Al termine del processo di modifica, le transazioni individuali possono essere caricate in CMDB attraverso l'opzione –lftwa.

Durante il caricamento degli elementi della configurazione nel database di gestione della configurazione, gli elementi della configurazione vengono sottoposti alla riconciliazione automatica che, se eseguita correttamente, restituisce dati di un singolo oggetto di business che aggiornano un singolo elemento della configurazione in CMDB. Durante il caricamento delle *transazioni degli elementi della configurazione* in TWA non viene eseguita alcuna riconciliazione automatica. È possibile che nell'area di lavoro transazione (TWA) compaiano diverse transazioni con attributi di identificazione destinati a un elemento della configurazione singolo. Le righe esistenti nell'area di lavoro transazione non vengono aggiornate quando vengono aggiunte nuove righe in modalità caricamento in TWA, anche se queste corrispondono a un elemento della configurazione esistente. Nell'area di lavoro transazione potrebbe persino apparire più volte definizioni identiche di elementi della configurazione.

GRLoader convalida i valori dei dati quando viene eseguito in modalità caricamento dalla modalità area di lavoro transazione (TWA) (-lftwa or -lftwai) per creare oggetti nel CMDB o quando viene eseguito utilizzando la modalità simulazione (-simci or –simrel). Vedere Modalità di simulazione di operazioni dell'area di lavoro transazione (TWA) (a pagina 671) per maggiori dettagli. I valori dei dati non vengono convalidati quando GRLoader viene eseguito nella modalità area di lavoro transazione (TWA) (-lttwa or -lttwar).

Il parametro -lttwai (o l'opzione di configurazione grloader.loadtotwa.inactivate) disattiva transazioni TWA caricate correttamente. Dopo che una transazione caricata correttamente è stata contrassegnata come disattiva, può essere eliminata in modo permanente dalla TWA utilizzando Archivia/Elimina.

Esempio: Carica in CMDB

Il seguente comando consente di caricare direttamente i dati in CMDB:

```
grloader … -i mydata.xml –a –n
```

Il file XML mydata.xml contiene:

```
<GRLoader>
  <ci>
     <name>server1</name>
     <class>Server</name>
   </ci>
</GRLoader>
```

Esempio: Carica in TWA

Il seguente comando consente di caricare i dati nell'area di lavoro transazione per la loro modifica prima del caricamento in CMDB:

```
grloader … -i mydata.xml -lttwa
```

Ulteriori informazioni:

Input XML (a pagina 668)
Ricerca (a pagina 668)
Formato data (a pagina 669)
EMPTY (a pagina 670)

Input XML

GRLoader utilizza dati di input XML. Durante il caricamento nell'area di lavoro transazione, le seguenti colonne XML vengono mappate per prevenire conflitti durante la sovrapposizione dei nomi delle colone con i nomi delle colonne standard nel database.

Nome XML DA	Colonna database A
tenant	tgt_tenant
id	tgt_id
delete_flag	tgt_delete_flag

Per le relazioni, le seguenti mappature ai applicano a::

Nome XML DA	Colonna database A
name	provider_name or dependent_name
dns_name	provider_dns_name or dependent_dns_name
delete_flag	tgt_delete_flag

Le mappature vengono invertite durante il caricamento dalle tabelle del database dell'area di lavoro transazione (TWA).

Ricerca

Quando si specificano dati per attributi di ricerca (SREL) nell'area di lavoro transizione, essi devono avere lo stesso formato come se fossero stati specificati in codice XML nativo per GRLoader. Gli attributi di ricerca accettano solo set di valori specifici che devono essere definiti in base a tabelle correlate in CA SDM. Questi attributi possono anche includere altre restrizioni ed eccezioni che devono essere soddisfatte ai fini dell'esecuzione dell'assegnazione. I valori specificati sono gli stessi indipendentemente che siano stati specificati in codice XML, SQL o nell'interfaccia Web dell'area di lavoro transazione.

Per stabilire se un attributo è un attributo SREL, consultare le seguenti sezioni della *Guida di riferimento tecnico di CA CMDB*:

- Famiglie e classi (sono identificati gli attributi SREL)
- Campi per contatti ed altre ricerche
- Campi convalidati in base ai dati di tabelle esistenti (SREL)

Esempio: XML di ricerca

Nel seguente esempio, la colonna alternativa SREL viene impostata specificando il parametro di ricerca:

```
<ci>
<name>server1</name>
<owner lookup="userid">mckpe99</owner>
</ci>
```

Nell'area di lavoro transazione, è possibile ottenere gli stessi risultati aggiungendo il suffisso del valore dei dati alla colonna SREL alternativa, separato da delimitatori (vedere grloader.workarea.delimiters sotto riportato). La transazione equivalente è rappresentata nell'area di lavoro transazione come di seguito:

ID	Nome	Proprietario
100	server1	mckpe99 {userid}

È inoltre possibile impostare il carattere delimitatore utilizzato in precedenza nel file di configurazione di GRLoader:

```
grloader.workarea.delimiters=xy
```

x e y sono caratteri diversi che di solito non appaiono nell'area di lavoro.

Formato data

GRLoader supporta le seguenti opzioni di formato data in XML:

- datefmt=UTC
- datefmt=ora locale (impostazione predefinita)

Esempi: XML datefmt

```
<ci>
<name>server1</name>
<purchase_date datefmt="UTC"> 1241197235</purchase_date>
</ci>
```

```
<ci>
<name>server3</name>
<purchase_date> 2009/05/01</purchase_date>
</ci>
```

La transazione equivalente è rappresentata nell'area di lavoro transazione come di seguito:

ID	Nome	purchase_date
101	server1	1241197235
102	server2	2009/05/01

Nota: se una data contiene un carattere speciale, ad esempio una barra (/), il formato è considerato come ora locale. Se una data non contiene caratteri speciali, la data è considerata come UTC.

EMPTY

GRLoader supporta l'opzione update_if_null in XML la quale cancella un campo in CMDB. Il seguente esempio riporta la cancellazione del campo Proprietario nel server1. Senza l'attributo, il campo Proprietario non viene coinvolto. Quando si utilizza l'area di lavoro transazione, può essere invece utilizzata la parola chiave EMPTY.

Esempio: XML update_if_null

```
<ci>
<name>server1</name>
<owner update_if_null="yes"></owner>
</ci>
```

Nell'area di lavoro transazione (TWA), il valore di database viene cancellato specificando la parola chiave EMPTY come valore di stringa. La transazione equivalente nell'area di lavoro è:

ID	Nome	Proprietario
102	server1	EMPTY

Il valore della parola chiave può essere impostato utilizzando l'opzione di configurazione grloader.emptyvalue:

```
grloader.emptyvalue=xxxx
```

xxxx rappresenta qualsiasi stringa che in genere non appare nei dati dell'area di lavoro.

Modalità di simulazione di operazioni dell'area di lavoro transazione (TWA)

È possibile predeterminare se un insieme di transazioni può creare nuovi elementi della configurazione (e pertanto creare nuove ambiguità per altri elementi della configurazione) utilizzando le seguenti opzioni:

–simci

Simula solo l'elaborazione delle transazioni degli elementi della configurazione. Permette di determinare se le transazioni creano o aggiornano gli elementi della configurazione. Quando si utilizza l'opzione -simci, GRLoader esegue una convalida dei dati.

–simrel

Simula solo l'elaborazione delle transazioni delle relazioni. Permette di determinare se le transazioni creano o aggiornano le relazioni. L'opzione –simrel verifica le relazioni controllando l'esistenza degli elementi della configurazione fornitore e dipendente, convalida i tipi di relazione e così via.

L'output della modalità simulazione è indirizzato all'area di lavoro transazione o al file _err.xml. In modalità di caricamento normale, il file the _err.xml contiene l'input dell'elemento della configurazione e un commento che indica se l'elemento della configurazione è stato inserito o aggiornato. Quando si utilizza la simulazione, il messaggio di GRLoader nella pagina Elenco Transazioni elemento della configurazione indica se l'elemento della configurazione o la relazione sono stati inseriti o aggiornati, con altri eventuali messaggi di errore. Lo stato della transazione rimane invariato.

È possibile attivare la simulazione in un file di configurazione utilizzando le opzioni **grloader.simulateloadci** e **grloader.simulateloadrelation**.

Nota: se l'input di GRLoader crea al contempo elementi della configurazione e relazioni, l'opzione –simrel può solo elaborare gli elementi della configurazione effettivi e non quelli pianificati per la creazione. A causa di questa limitazione, le opzioni -simci e –simrel si escludono a vicenda.

Modalità di utilizzo SQL per aggiornare i dati nell'area di lavoro transazione (TWA)

L'area di lavoro transazione (TWA) è archiviata in MDB ed è possibile aggiornarla direttamente con query SQL.

Ulteriori informazioni:

Tabelle TWA (a pagina 672)
Nomi delle colonne di TWA SQL (a pagina 673)
Inserimento di nuovi record in TWA (a pagina 675)
Modalità di utilizzo del driver ODBC (a pagina 676)
Identificativi degli elementi della configurazione nell'area di lavoro transazione (TWA) (a pagina 676)
Modalità di impostazione dello stato della transazione (a pagina 677)
Modalità di condivisione delle tabelle con CA SDM (a pagina 677)

Tabelle TWA

Le tabelle dell'area di lavoro transazione (TWA) includono:

ci_twa_ci

Singola tabella che contiene tutti gli attributi di tutte le famiglie di elementi della configurazione. I dati di questa tabella vengono archiviati in modo denormalizzato per consentire agli utenti e ai servizi di comprendere e modificare il contenuto.

ci_twa_relation

Complemento della tabella the ci_twa_ci. La tabella contiene le informazioni sulle relazioni con gli elementi della configurazione.

I nomi delle colonne dell'area di lavoro transazione corrispondono agli attributi utilizzati con GRLoader, con qualche eccezione.

Nota: per informazioni sugli attributi dell'elemento della configurazione, consultare la *Guida di riferimento tecnico di CA CMDB*.

Nomi delle colonne di TWA SQL

I nomi delle colonne nelle tabelle ci_twa_ci e ci_twa_relation corrispondono ai nomi degli attributi Elemento della configurazione e Relazione con alcune eccezioni.

Campi di TWA comuni a ci_twa_ci e ci_twa_relation

apply_after_dt (Applica Dopo la data)

GRLoader esegue la transazioni solo se la data attuale è successiva a quella indicata in Applica dopo la data. Il campo funziona in termini di secondi a partire dalla data indicata. Se il valore riportato è zero (0), il campo viene ignorato.

tran_chg_ref_num (Ordine di cambiamento)

Specifica l'identificatore dell'ordine di cambiamento associato alla transazione. L'opzione GRLoader –chg utilizza questo attributo per selezionare solo le transazioni con un numero di ordine di cambiamento specifico.

Nota: per ulteriori informazioni sull'uso dell'opzione –chg, consultare Filtra per numero di ordine di cambiamento (a pagina 684).

tran_status (Stato transazione)

Specifica che lo stato della transazione deve essere uno dei seguenti valori (vengono eseguite solo le transazioni con tran_status=1).

Valore	Descrizione breve	Descrizione estesa
0	Iniziale	Valore predefinito. Richiede l'impostazione dell'intervento su "Pronto" per consentire a GRLoader di lavorare su questa transazione.
1	Pronto	La transazione è pronta per essere caricata nell'elemento della configurazione appropriato o nelle tabelle di relazione
2	Riuscito	La transazione è stata elaborata correttamente
3	Avviso	Avviso rilevato durante il caricamento in ca_owned_resource/bmhier
4	Errore	Errore rilevato durante il caricamento in ca_owned_resource/bmhier
40000+	Ad uso dell'utente	

tran_message (Messaggio)

Messaggio GRLoader che mostra i risultati del caricamento o della simulazione.

tran_dt (Data transazione)

Impedisce che le i dati della transazione precedenti si sovrappongono accidentalmente su quelli attuali. La data della transazione viene confrontata con la data dell'ultima modifica dell'elemento della configurazione e GRLoader rifiuta la transazione se l'elemento della configurazione è più recente.

Se GRLoader rifiuta una transazione perché precedente all'elemento della configurazione di destinazione, verificare che la transazione sia applicabile, impostare manualmente la data della transazione su una data più recente e riavviare GRLoader.

tgt_delete_flag (Attivo)

Disattiva l'elemento della configurazione di destinazione o la relazione. Impostare il valore su 1 (uno). L'impostazione del valore delete_flag su 1 ha un significato diverso in quanto indica che la transazione deve essere eliminata.

Colonne ci_twa_ci

Oltre ai nomi delle colonne descritti di seguito, è possibile anche impostare i nomi per gli attributi dell'elemento della configurazione sui nomi delle colonne utilizzati nelle istruzioni SQL.

tgt_id (Elemento della configurazione di destinazione)

Specifica l'UUID dell'elemento della configurazione di destinazione. Usato durante la riconciliazione manuale.

superseded_by (Sostituito da)

Specifica l'UUID dell'elemento della configurazione sostituito.

tgt_tenant (titolare)

Consente di specificare il nome titolare assegnato all'elemento della configurazione di destinazione. Il titolare può essere assegnato all'elemento della configurazione solo al momento della creazione di quest'ultimo se l'utente GRLoader dispone delle autorizzazioni adeguate. Applicabile solo se Multi-Tenancy è attivato.

Colonne ci_twa_relation

Oltre ai nomi delle colonne descritti di seguito, è possibile anche impostare i nomi per gli attributi dell'elemento della configurazione sui nomi delle colonne utilizzati nelle istruzioni SQL.

Quando si utilizza SQL è possibile usare i seguenti nomi di colonne del database per definire le transazioni delle relazioni:

provider_name (Nome fornitore)

provider_mac_address (Indirizzo MAC fornitore)

provider_serial_number (Numero di serie fornitore)

provider_system_name (Nome host fornitore)

provider_asset_num (Numero asset fornitore)

provider_dns_name (Nome DNS fornitore)

provider_tenant (Titolare fornitore)

E

dependent_name (Nome dipendente)

dependent _mac_address (Indirizzo MAC dipendente)

dependent _serial_number (Numero di serie dipendente)

dependent _system_name (Nome Host dipendente)

dependent _asset_num (Numero asset dipendente)

dependent _dns_name (Nome DNS dipendente)

dependent_tenant (Titolare dipendente)

Se è noto l'UUID dell'elemento della configurazione fornitore o di quello dipendente, è possibile utilizzare i seguenti campi:

provider_id specifica l'UUID dell'elemento della configurazione fornitore

dependent_id specifica l'UUID dell'elemento della configurazione dipendente

Nota: provider_tenant e dependent_tenant si applicano solo quando è abilitata la multi-tenancy.

Inserimento di nuovi record in TWA

È possibile inserire un nuovo record nelle tabelle ci_twa_ci e ci_twa_relation esternamente a CA SDM.

Per inserire record nelle tabelle ci_twa_ci e ci_twa_relation, inserire 0 nella colonna ID effettuando le seguenti operazioni:

```
Inserire nei valori ci_twa_ci (id, nome) i valori (0,'test-ci')
inserire nei valori ci_twa_relation (id, tipo) i valori (0,'test-relation-type')
```

Attenzione: se Multi-Tenancy è attivato, è necessario specificare gli attributi del titolare, ovvero tenant, tgt_tenant, provider_tenant o dependent_tenant appropriati. Se si creano transazioni TWA senza specificare un titolare, viene utilizzato il titolare Pubblico.

Modalità di utilizzo del driver ODBC

È possibile utilizzare SQL invece di GRLoader per il caricamento dei dati nell'area di lavoro transazione. Si consiglia di utilizzare il driver ODBC fornito con CA SDM, anziché servizi SQL nativi. Con l'utilizzo del driver ODBC, è possibile ottenere i seguenti benefici:

- Prestazioni
- Protezione
- Indipendenza del database
- Integrità dei dati in un ambiente in cui potrebbero verificarsi degli aggiornamenti del database provenienti dal server di CA SDM contemporanei all'esecuzione dello strumento di modifica in blocco.

Avvertenze

- Solo i driver ODBC di CA SDM offrono funzionalità di protezione, quali multi-tenancy, partizione dei dati e accesso basato su ruoli. Nessun protezione viene invece applicata se SQL viene eseguito attraverso i driver DBMS nativi.
- Si consiglia di eseguire frequenti backup dei dati durante gli aggiornamenti eseguiti utilizzando SQL nativo.

Identificativi degli elementi della configurazione nell'area di lavoro transazione (TWA)

Nella tabella ci_twa_ci, tre identificatori sono associati con una transazione dell'elemento della configurazione: ID, tgt_id e superseded_by. Questi attributi sono i seguenti:

- ID corrisponde al numero di sequenza della transazione. **Non modificare questo campo.** Gli ID 1-2.000.000.000 sono destinati all'uso da parte dei sistemi che modificano l'area di lavoro transazione al di fuori del server di CA SDM. Gli ID da 2.000.000.001 a circa 4.000.000.000 sono destinati all'uso da parte di CA SDM. All'esaurimento degli ID, reinizializzare la tabella.
- tgt_id, provider_id o dependent_id rappresentano l'UUID dell'elemento della configurazione di destinazione. Impostare questo campo ogni volta che si esegue la riconciliazione manuale.
- superseded_by è l'UUID dell'elemento della configurazione sostitutivo. Impostare questo campo ogni volta che si designa manualmente l'elemento della configurazione sostitutivo per la transazione.

Modalità di impostazione dello stato della transazione

È possibile impostare lo stato (tran_status) di ogni transazione presente nell'area di lavoro transazione (TWA). Affinché GRLoader sia in grado di elaborare una transazione, è necessario impostare lo stato su Pronto (tran_status=1).

Valore	Descrizione breve	Descrizione estesa
0	Iniziale	Valore predefinito. Deve essere impostato su "Pronto" dall'utente per consentire a GRLoader di lavorare su questa transazione.
1	Pronto	La transazione è pronta per essere caricata nell'elemento della configurazione appropriato o nelle tabelle di relazione
2	Riuscito	La transazione è stata elaborata correttamente
3	Avviso	Avviso rilevato durante il caricamento in ca_owned_resource/bmhier
4	Errore	Errore rilevato durante il caricamento in ca_owned_resource/bmhier
40000+	Ad uso dell'utente	

Se GRLoader –lftwa viene eseguito due o più volte, lo stato viene aggiornato quando, in seguito alla prima e alle successive esecuzioni, non viene rilevata alcuna transazione. Reimpostare lo stato della transazione pronta prima di ogni esecuzione di –lftwa di GRLoader.

Per informazioni su come rappresentare i dati XML nelle tabelle dell'area di lavoro transazione (TWA), vedere gli esempi XML riportati nelle sezioni precedenti.

Modalità di condivisione delle tabelle con CA SDM

Solo SQL Server

Quando si utilizza SQL per aggiornare le tabelle ci_twa_ci e ci_twa_relation, impostare manualmente la colonna last_mod_dt come riportato di seguito:

```
SET last_mod_dt = DATEDIFF(s,'19700101', GETUTCDATE())
```

Esempio: Set last_mod_dt

Nell'esempio riportato di seguito viene impostato last_mod_dt:

```
UPDATE ci_twa_ci
        SET tran_status=1,
                last_mod_dt = DATEDIFF(s,'19700101', GETUTCDATE())
        WHERE tran_status=1
```

Nota: gli aggiornamenti delle tabelle dell'area di lavoro transazione potrebbero richiedere alcuni minuti prima di venire visualizzati nell'interfaccia Web o in GRLoader. Per ulteriori informazioni sui tempi di aggiornamento, vedere l'opzione NX_DBMONITOR_TIMER_MINUTES.

Modalità di utilizzo dell'interfaccia Web per aggiornare i dati nell'area di lavoro transazione (TWA)

Prima dell'esecuzione è possibile verificare le transazioni per elementi della configurazione e di relazione copiando i dati nell'area a gestione temporanea dell'area di lavoro transazione (TWA). Una volta nell'area a gestione temporanea, è possibile manipolare gli elementi della configurazione e le relazioni utilizzando l'interfaccia Web.

È anche possibile convalidare le transazioni degli elementi di configurazione e di relazione per impedire la creazione di dati non validi o nuovi elementi di configurazione quando avrebbero dovuto essere aggiornati elementi della configurazione singoli o esistenti. Con questo approccio è possibile visualizzare ogni transazione e gli elementi della configurazione potenziali che può aggiornare in modo da poter riconciliare manualmente la transazione con l'elemento della configurazione di destinazione.

Per gestire l'area di lavoro transazione, selezionare la scheda Amministrazione e passare al nodo CA CMDB, Area di lavoro transazione. Da questo nodo è possibile gestire le pagine dell'area di lavoro transazione.

Nota: per ulteriori informazioni, consultare la *Guida in linea*.

Ulteriori informazioni:

Gestione delle transazioni di elementi della configurazione (a pagina 679)
Gestione di transazioni di elementi della configurazione ambigui (a pagina 680)
Riconciliazione manuale (a pagina 680)

Gestione delle transazioni di elementi della configurazione

Nella pagina Dettagli transazione elemento della configurazione vengono visualizzati tutti gli attributi non vuoti della transazione. Se si deseleziona la casella Nascondi valori vuoti, verranno visualizzati tutti gli attributi degli elementi della configurazione. Per informazioni aggiuntive su un attributo, posizionare il puntatore sul nome dell'attributo.

È possibile effettuare le seguenti operazioni:

- Visualizzare una transazione
- Creare una transazione
- Modificare la transazione
- Salvare o annullare modifiche della transazione (modalità Modifica)
- Reimpostare i dati originali della transazione (modalità Modifica)
- Mostrare o nascondere dati (scheda Attributi)
- Impostare l'elemento della configurazione di destinazione (scheda Riconciliazione)

Dopo aver salvato una transazione singola, selezionare la scheda Riconciliazione di tale transazione per verificare che non ci siano ambiguità nell'elemento della configurazione di destinazione specificato. Se è presente un'ambiguità, è possibile specificare un elemento della configurazione di destinazione (a pagina 663). Dopo aver inserito tutti i dati richiesti, è possibile simulare il caricamento dei dati (a pagina 671) per validare i dati e controllare la riconciliazione.

Importante Per l'immissione dei dati nell'area di lavoro della transazione mediante questa interfaccia Web, attenersi alle regole descritte nella sezione Modalità di caricamento dati nell'area di lavoro della transazione (TWA) con GRLoader (a pagina 666).

L'interfaccia Web non convalida i dati con distinzione maiuscole/minuscole nell'area di lavoro della transazione. Verificare che i valori immessi coincidano esattamente con i valori ricercati. In alternativa, all'avvio di GRLoader, è possibile specificare l'opzione –I per abilitare la ricerca senza distinzione maiuscole/minuscole.

Nota: anche se tgt_id o superseded_by vengono memorizzati come UUID nella transazione, vengono comunque visualizzati come nomi degli elementi della configurazione nell'interfaccia Web.

Gestione di transazioni di elementi della configurazione ambigui

È possibile rivedere e modificare transazioni che hanno elementi della configurazione di destinazione ambigui prima di caricare i dati delle transazioni. È inoltre possibile risolvere transazioni per elementi della configurazione che non hanno un elemento della configurazione di destinazione ma hanno attributi identificativi per uno o più elementi della configurazione. Questa risoluzione garantisce che venga aggiornato l'elemento della configurazione appropriato ed evita la creazione di dati errati e incoerenti.

Dopo aver salvato una transazione singola, selezionare la scheda Riconciliazione di tale transazione per verificare che non ci siano ambiguità nell'elemento della configurazione di destinazione specificato. Se è presente un'ambiguità, è possibile specificare un elemento della configurazione di destinazione (a pagina 663). Dopo aver inserito tutti i dati richiesti, è possibile simulare il caricamento dei dati (a pagina 671) per validare i dati e controllare la riconciliazione.

Per ulteriori informazioni sulla riconciliazione dei dati in TWA, vedere Revisione e modifica dei dati entranti tramite TWA (Transaction Work Area) (a pagina 657).

Riconciliazione manuale

Per eseguire la riconciliazione manuale della transazione di un elemento della configurazione, determinare l'elemento della configurazione di destinazione che corrisponde agli attributi di identificazione della transazione e impostare il campo tgt_id della transazione sull'UUID dell'elemento della configurazione di destinazione.

Quando GRLoader elabora una transazione che specifica un campo tgt_id, viene eseguito l'aggiornamento dell'elemento della configurazione di destinazione con le informazioni della transazione e viene nuovamente registrato l'elemento della configurazione se i rispettivi attributi di identificazione sono stati modificati.

È possibile specificare l'elemento della configurazione di destinazione in modo esplicito nella transazione. È anche possibile utilizzare la scheda Riconciliazione per selezionare un elemento della configurazione di destinazione.

Per ulteriori informazioni, consultare Revisione e modifica dei dati in entrata tramite TWA (Transaction Work Area) (a pagina 657).

Definizione di un elemento della configurazione di destinazione per una transizione dell'elemento della configurazione ambigua

È possibile specificare un elemento della configurazione per una transazione ambigua in modo che i dati vengano indirizzati a un elemento della configurazione di destinazione specifico, indipendentemente dai valori di identificazione specificati nella transazione.

Per specificare un elemento della configurazione di destinazione per una transazione dell'elemento della configurazione ambigua:

1. Selezionare una transazione dell'elemento della configurazione nella pagina Elenco Transazioni ambigue.

   Viene visualizzata la pagina dei dettagli della transizione dell'elemento della configurazione.

2. Fare clic su Modifica.

   Viene visualizzata la pagina Aggiorna elemento della configurazione.

3. Nella scheda Riconciliazione selezionare un elemento della configurazione dall'elenco per impostare l'elemento della configurazione come elemento della configurazione di destinazione per la transazione. Fare clic su Imposta destinazione, quindi fare clic su Salva.

   L'elemento della configurazione selezionato diventa quello di destinazione per la transazione.

Gestione di transazioni di relazione

Nell'elenco delle transazioni di relazione vengono visualizzate gli input dei dati della transazione di relazione.

In questa pagina è possibile effettuare le seguenti operazioni:

- Eseguire ricerche di transazioni di elementi della configurazione

Nell'elenco, è possibile effettuare le seguenti operazioni:

- Creare una transazione di relazione
- Effettuare modifiche nell'elenco (eccetto l'identificazione di attributi)

Aggiornamento di una transazione di relazione

È possibile visualizzare e modificare i dati di un'unica transazione di relazione. Nella pagina Dettagli transazione relazione, è possibile effettuare le seguenti operazioni:

- Creare una transazione di relazione
- Visualizzare la transazione

- Modificare la transazione
- Salvare o annullare modifiche della transazione (modalità Modifica)
- Reimpostare i dati originali della transazione (modalità Modifica)

Per aggiornare una transazione di relazione

1. Fare clic su Modifica.

   Viene visualizzata la pagina Aggiorna transazione relazione.

2. Modificare e compilare i campi.
3. Selezionare Attivo.
4. Fare clic su Salva.

   La transazione di relazione viene salvata.

Dopo aver inserito tutti i dati richiesti, è possibile simulare il caricamento dei dati per validare i dati e controllare la riconciliazione.

Importante Per l'immissione dei dati nell'area di lavoro della transazione mediante questa interfaccia Web, attenersi alle regole descritte nella sezione Modalità di caricamento dati nell'area di lavoro della transazione (TWA) con GRLoader (a pagina 666).

L'interfaccia Web non convalida i dati con distinzione maiuscole/minuscole nell'area di lavoro della transazione. Verificare che i valori immessi coincidano esattamente con i valori ricercati. In alternativa, all'avvio di GRLoader, è possibile specificare l'opzione –I per abilitare la ricerca senza distinzione maiuscole/minuscole.

Nota: anche se provider_id o dependent_id vengono memorizzati come UUID nella transazione, vengono comunque visualizzati come nomi degli elementi della configurazione nell'interfaccia Web.

Modalità di caricamento delle transazioni in CMDB

Anziché utilizzare input XML per la creazione di elementi della configurazione e relazioni, è possibile specificare le seguenti opzioni per selezionare l'area di lavoro transazione (TWA) come origine dell'input:

–lftwa (carica da TWA)

–lftwai (carica da TWA e disattiva)

Nota: diversamente da altre modalità di GRLoader che utilizzano il file err.xml, il caricamento dalla TWA restituisce al campo Messaggio della transazione messaggi di errore per la visualizzazione.

Al completamento dell'elaborazione delle transazioni, GRLoader imposta lo stato delle transazioni per indicare lo stato Riuscito o Non riuscito di ogni transazione in TWA. Se l'opzione -lftwa di GRLoader viene eseguita più volte consecutivamente, è necessario impostare lo stato della transazione su Pronto tra le varie esecuzioni di GRLoader, poiché quest'ultimo non tenta di caricare dati già caricati.

La transazione viene eseguita dall'area di lavoro transazione come se GRLoader fosse stato eseguito attraverso un input XML. La protezione della transazione si basa sull'utente che esegue il caricamento dall'area di lavoro transazione, e non sull'utente che ha eseguito originariamente il caricamento della transazione dell'area di lavoro.

L'audit verrà effettuato al corretto completamento dell'elaborazione delle transazioni.

Nota: prima di eseguire il caricamento, è possibile predeterminare se una serie di transazioni creerà nuovi elementi della configurazione o relazioni utilizzando le opzioni di simulazione (-simci e -simrel). Vedere Modalità di simulazione di operazioni dell'area di lavoro transazione (TWA) (a pagina 671) per ulteriori informazioni.

Ulteriori informazioni:

Prevenzione della regressione di dati (a pagina 683)
Filtro per numero di un ordine di cambiamento (a pagina 684)

Prevenzione della regressione di dati

Mentre i dati delle transazioni per un elemento della configurazione sono nell'area di lavoro transazione (TWA), altre azioni possono aggiornare tale elemento della configurazione in CMDB e provocare l'invalidità dei dati delle transazioni nell'area di lavoro transazione. Per impedire una regressione di dati non desiderata, GRLoader confronta il campo tran_dt (Data transazione) dell'area di lavoro transazione (TWA) con last_update_dt (Data ultima modifica) o relazione last_mod_dt (Data ultima modifica) dell'elemento della configurazione. Se last_update_dt è più recente, GRLoader rifiuta la transazione TWA e registra un messaggio di errore nella colonna tran_message.

È possibile risolvere questa situazione effettuando una delle seguenti operazioni:

- Utilizzare l'interfaccia Web per modificare il campo tran_dt dell'elemento della configurazione o della relazione (Data transazione) con un valore più appropriato.
- Impostare l'opzione GRLoader grloader.workarea.ignore_transaction_dates="yes" per ignorare le date delle transazioni e inserire i dati.

Nota: se GRLoader rifiuta una transazione perché precedente all'elemento della configurazione di destinazione, e successivamente si accerta che la transazione deve essere eseguita, impostare manualmente la data della transazione sulla data corrente e riavviare GRLoader.

Avviso: Le date relative all'opzione che ignora la transazione possono causare lo spostamento di livello o la regressione dei dati. Quando un singolo elemento della configurazione o relazione viene più volte aggiornato nella stessa esecuzione dell'opzione GRLoader -lftwa, la data dell'ultimo aggiornamento (last_update) dell'elemento della configurazione o relazione viene impostata alla data corrente durante il primo aggiornamento. Per consentire più aggiornamenti dello stesso elemento della configurazione o relazione, viene eseguito un controllo aggiuntivo per verificare che sia stato aggiornato l'elemento della configurazione o la relazione dopo l'avvio di GRLoader. Se è stato aggiornato, l'aggiornamento è consentito.

Filtro per numero di un ordine di cambiamento

L'opzione di GRLoader -chg può essere utilizzata per selezionare solo le transazioni associate a un ticket di cambiamento. Per filtrare per numero di cambiamento, è necessario impostare l'attributo Ordine di cambiamento (tran_chg_ref_num) sul numero appropriato di richiesta di cambiamento.

Nota: la stringa Ordine di cambiamento non è convalidata quando viene caricata in CMDB.

Esempio: filtro per ticket di cambiamento

La seguente opzione consente di caricare solo le transazioni associate all'ordine di cambiamento 23434.

```
grloader -lftwa -chg 23434
```

Amministrazione dell'area di lavoro transazione (TWA)

L'area di lavoro transazione (TWA) può richiedere la seguente gestione:

- Estensione dell'area di lavoro transazione (TWA) – richiesta quando si estende una qualsiasi famiglia OOB o si definiscono le proprie famiglie personalizzate.
- Archiviazione ed eliminazione dell'area di lavoro transazione (TWA)
- Modalità di utilizzo dell'area di lavoro transazione (TWA) con CA Cohesion ACM
- Limitazioni del database

Ulteriori informazioni:

Estensione dell'oggetto TWA (a pagina 685)
Archiviazione ed eliminazione dell'area di lavoro transazione (TWA) (a pagina 686)
Opzioni di comando GRLoader dell'area di lavoro transazione (TWA) (a pagina 686)
Opzioni del file di configurazione GRLoader dell'area di lavoro transazione (TWA) (a pagina 687)
Modalità di utilizzo dell'area di lavoro transazione (TWA) con CA Cohesion ACM (a pagina 688)
Limitazioni del database (a pagina 688)

Estensione dell'oggetto TWA

Qualsiasi modifica apportata allo schema della famiglia di CA CMDB richiede delle modifiche parallele nello schema TWA. Se non sono stati aggiunti attributi o famiglie personalizzate, non è necessario apportare modifiche nella TWA.

Per estendere l'oggetto TWA

1. Personalizzare le famiglie e gli attributi definiti dall'utente attraverso le procedure di estensione di CA CMDB descritte nella *Guida all'amministrazione*.
2. Aggiungere gli attributi della nuova famiglia allo schema ci_twa_ci utilizzando Progettazione schema di WSP (Web Screen Painter Schema Designer).

   Per aggiungere un nuovo attributo allo schema ci_twa_ci:

   1. Attraverso Progettazione schema di WSP, aprire lo schema per la tabella ci_twa_ci.
   2. Aggiungere l'attributo della famiglia desiderato alla tabella estensioni.
   3. Pubblicare lo schema ci_twa_ci modificato.

   Nota: il nuovo attributo deve essere di tipo STRING e possedere il maggior valore del testo possibile.
3. Aggiungere i metadati per la famiglia personalizzata nella TWA come riportato di seguito:
   1. Utilizzando Web Screen Painter, aprire il cmdb_metadata_site_families.htmpl.
   2. Aggiungere PDM_INCLUDE per il file cmdb_metadata_*extension*.htmpl creato per la personalizzazione della famiglia.

Archiviazione ed eliminazione dell'area di lavoro transazione (TWA)

Per gestire l'area di lavoro transazione, sono disponibili le seguenti regole di archiviazione ed eliminazione:

Trans elem config non att

Archivia ed elimina transazioni per elementi della configurazione contrassegnate per l'eliminazione.

Trans elem config corrett

Archivia ed elimina transazioni per elementi della configurazione eseguite correttamente.

Trans relaz non attive

Archivia ed elimina transazioni di relazione contrassegnate per l'eliminazione.

Trans relaz corrette

Archivia ed elimina transazioni di relazione eseguite correttamente.

È possibile specificare la frequenza con cui vengono eseguite le regole o se sono attivate.

È possibile personalizzare e attivare le regole per attivare l'archiviazione e l'eliminazione dell'area di lavoro transazione (TWA). Se si utilizza l'area di lavoro transazione (TWA) in modo intensivo, fare attenzione ai limiti del numero di record nella TWA imposti dal DBMS.

Se è necessario reinizializzare l'area di lavoro transazione (TWA) per cancellare tutti i dati relativi, effettuare una delle azioni seguenti:

- Impostare tutte le transazioni come inattive
- Eseguire l'eliminazione dell'archivio

Importante! Non utilizzare SQL per eliminare tutti i record dell'area di lavoro transazione (TWA) poiché elimina i record dell'intestazione necessari.

Opzioni di comando GRLoader dell'area di lavoro transazione (TWA)

CA SDM fornisce le seguenti opzioni di comando da utilizzare nell'elaborazione dell'area di lavoro transazione (TWA) di GRLoader:

-lttwa

Carica dati XML nello stato iniziale.

-lttwar

Carica dati XML nello stato pronto.

-lftwa

Carica transazioni dalla TWA.

-lftwai

Carica transazioni dalla TWA e disattiva transazioni riuscite.

-chg *nnnn*

Utilizzata con –lftwa e -lftwar. Carica solamente le transazioni associate a un ordine di cambiamento *nnnn*.

Nota: la stringa Ordine di cambiamento non è convalidata quando viene caricata in CMDB.

-I

Ignorare la distinzione tra maiuscole e minuscole per gli attributi di ricerca. Per impostazione predefinita, il testo a mano libera degli attributi di ricerca viene elaborato facendo distinzione tra maiuscole e minuscole a meno che non venga utilizzata questa opzione.

-simci

Determina se le transazioni degli elementi della configurazione possono creare o aggiornare elementi della configurazione. Quando di utilizza questa opzione, GRLoader esegue il controllo degli errori solo per l'elemento della configurazione.

-simrel

Determina se le transazioni di relazione possono creare o aggiornare relazioni. Questa opzione verifica le relazioni per l'esistenza del provider e gli elementi della configurazione dipendenti, inoltre convalida i tipi di relazione ecc.

Opzioni del file di configurazione GRLoader dell'area di lavoro transazione (TWA)

CA CMDB offre le seguenti opzioni dell'area di lavoro transazione (TWA) per il file di configurazione di GRLoader:

grloader.emptyvalue=EMPTY

grloader.loadfromtwa=yes

grloader.loadfromtwa.inactivatesuccessful=yes/no

grloader.loadtotwa=yes

grloader.loadtotwa.ready=yes/no

grloader.workarea.delimiters={ }

grloader.workarea.ignore_transaction_dates=yes

grloader.simulateloadci=yes/no

grloader.simulateloadrelation=yes/no

Modalità di utilizzo dell'area di lavoro transazione (TWA) con CA Cohesion ACM

Per utilizzare TWA con CA Cohesion ACM, applicare la patch RO08739 a CA Cohesion ACM r5. Questa patch consente di specificare l'opzione –lttwa nel campo Other Options della scheda Export Options della definizione Export Report di CA CMDB. Aggiornare il componente GRLoader. Contattare il supporto di CA per domande.

Limitazioni del database

La TWA è soggetta a limitazioni dei dati imposte dal database utilizzato:

- Quando si utilizza l'area di lavoro transazione (TWA) e Microsoft SQL Server, la lunghezza totale di una transazione dati non deve superare 8060 byte.
- Quando si utilizzano le utilità dbload e pdm_load, l'operazione di caricamento è limitata a 512 colonne.
- Il limite di colonne per Oracle è 1000. Se si procede ad una personalizzazione del proprio CA CMDB, verificare che il numero totale di attributi non superi il totale di 1000 fra tutte le famiglie (fornite da CA e definite dall'utente).
- I limiti per SQL Server 2005 vengono descritti nella tabella seguente:

Tipo di limitazione	Limite (32 bit e 64 bit)
Colonne per tabella estesa in larghezza	30000
Colonne per tabella di base	1024
Colonne per istruzione SELECT	4096
Byte per riga	8060
Righe per tabella	Limitato dalla capacità di archiviazione disponibile

Manutenzione dei dati di CA CMDB

Le operazione di manutenzione dei dati di CMDB richiedono privilegi di amministratore. Tali operazioni includono l'impostazione di famiglie, classi e tipi di relazione per la gestione degli elementi della configurazione e delle informazioni sulle relazioni.

Ulteriori informazioni:

Struttura delle classi/famiglie di CA CMDB (a pagina 689)
Modifica della famiglia/classe di un singolo elemento della configurazione (a pagina 690)
Modifica della famiglia/classe di un elenco di elementi della configurazione (a pagina 690)
Modifica della famiglia/classe di elementi della configurazione con GRLoader (a pagina 691)
Estensione di CA CMDB (a pagina 691)

Struttura delle classi/famiglie di CA CMDB

CA CMDB fornisce famiglie di elementi della configurazione predefinite e classi degli elementi della configurazione in esse contenuti.

Nota: per informazioni sulle strutture delle classi e delle famiglie CA CMDB predefinite, vedere la *Guida di riferimento tecnico CA CMDB*.

Nota: le seguenti famiglie di base di Service Desk e CA APM non dispongono delle proprie tabelle di estensioni di CA CMDB:

- Computer
- Contatto (come oggetto base)
- Hardware
- Posizione (come oggetto base)
- Organizzazione (come oggetto base)
- Altro
- Progetto
- Software

In CA CMDB gli elementi della configurazione delle famiglie base ricevono pagine di dettagli di elementi della configurazione con alcuni campi estranei e senza alcuna scheda Attributi. Per sfruttare i vantaggi offerti dalle funzioni avanzate di CA CMDB, quali la possibilità di tenere traccia di attributi specifici delle famiglie, il controllo delle versioni nonché snapshot e linee di base, è consigliabile utilizzare la funzionalità per la modifica di classi e famiglie per convertire questi elementi della configurazione in famiglie CA CMDB.

Modifica della famiglia/classe di un singolo elemento della configurazione

È possibile modificare la famiglia e la classe di un singolo elemento della configurazione.

Per modificare la famiglia e la classe di un singolo elemento della configurazione

1. Selezionare l'elemento della configurazione che si desidera modificare.
2. Fare clic su Modifica.

   Viene visualizzata la pagina Aggiorna elemento della configurazione.
3. Modificare il valore Classe dell'elemento della configurazione. La selezione della classe determina anche la famiglia dell'elemento della configurazione. È possibile immettere un valore direttamente o fare clic sulla lente di ingrandimento per selezionarne uno dall'elenco di classi.
4. Fare clic su Salva.

   La famiglia e la classe del singolo elemento della configurazione sono state modificate.

Modifica della famiglia/classe di un elenco di elementi della configurazione

È possibile modificare la famiglia e la classe di un elenco di elementi della configurazione.

Per modificare la famiglia/classe di un elenco di elementi della configurazione

1. Nella pagina Elenco elementi della configurazione fare clic su Mostra filtro.
2. Compilare uno o più campi di ricerca per cercare gli elementi della configurazione da modificare.
3. Fare clic su Cerca.

   Nell'Elenco elementi della configurazione vengono inseriti tutti gli elementi della configurazione che corrispondono ai criteri di ricerca.
4. Fare clic su Modifica nell'elenco.

   L'Elenco elementi della configurazione visualizza i campi che è possibile modificare per tutti gli elementi della configurazione selezionati.
5. Modificare i campi Famiglia e Classe come desiderato.
6. Fare clic su Modifica tutto.
7. Fare clic su Salva.

   Quando si aggiorna l'Elenco elementi della configurazione, vengono visualizzati gli elementi della configurazione aggiornati.

Modifica della famiglia/classe di elementi della configurazione con GRLoader

È possibile modificare la famiglia e la classe di elementi della configurazione utilizzando GRLoader.

Per modificare la famiglia/classe di un elemento della configurazione con GRLoader

1. Creare il codice XML per modificare l'attributo dell'elemento della configurazione.
2. Utilizzando GRLoader, aprire l'elemento della configurazione che si desidera modificare.
3. Eseguire il codice XML tramite GRLoader per modificare l'attributo dell'elemento della configurazione.

   La famiglia e la classe dell'elemento della configurazione sono state modificate.

Esempio: Impostazione della classe di un elemento della configurazione aperto su Documento

Il seguente esempio mostra un frammento di codice XML che imposta la classe di un elemento della configurazione aperto su *Documento*.

```
<ci>
    Numero documento<name> 1
    <class>Documento
<ci>
```

Importante Non tentare di aggiornare contemporaneamente gli attributi Famiglia e Classe. Per modificarli entrambi, è necessario utilizzare due aggiornamenti separati degli elementi della configurazione in due attivazioni di GRLoader distinte.

Estensione di CA CMDB

<cmdb> è un sistema estremamente flessibile che può essere esteso in modo tale da contenere altre famiglie, classi e attributi secondo le esigenze di business. I nuovi attributi possono essere specifici delle famiglie o *comuni*, ovvero applicabili a tutte le famiglie. Sebbene CA CMDB fornisca famiglie predefinite con numerose classi e attributi basati su standard di settore, in alcuni casi è necessario effettuare almeno una delle seguenti operazioni:

- Estendere una o più famiglie di elementi della configurazione mediante l'aggiunta di nuovi attributi. Ad esempio, per aggiungere le coordinate GPS per ogni dispositivo di un'università, si può definire l'attributo gps_coordinate per aggiungerlo a qualsiasi famiglia desiderata. Se è necessario estendere solo una famiglia, utilizzare Progettazione schema di Web Screen Painter per definire i nuovi attributi nella tabella estensioni esistente. Inoltre, quando si aggiunge un attributo, occorre modificare anche la pagina Dettagli, la scheda Attributo e i moduli di metadati che utilizzano l'attributo. Per ulteriori informazioni, vedere Aggiunta di attributi delle famiglie (a pagina 693).

- Estendere tutte le famiglie di elementi della configurazione aggiungendo un attributo comune. Per ulteriori informazioni, vedere Aggiunta di attributi comuni (a pagina 694).
- Aggiungere nuove classi a una famiglia esistente per avere una classificazione più dettagliata nel sistema. Ad esempio, invece della classe generica Server, si può creare una classe a parte per ogni modello di dispositivo server. Per ulteriori informazioni, vedere Definizione di una nuova classe di elementi della configurazione (a pagina 695).
- Aggiungere una nuova famiglia utilizzando una tabella estensioni esistente e i suoi attributi. Specificare una nuova famiglia è un metodo alternativo per organizzare o classificare gli elementi della configurazione. Per ulteriori informazioni, vedere Definizione di una nuova famiglia di elementi della configurazione (a pagina 695).
- Se la struttura esistente di classi o famiglie non soddisfa le proprie esigenze, è possibile crearne di nuove utilizzando un numero ridotto di attributi. Se si desidera aggiungere una nuova famiglia utilizzando una nuova tabella estensioni, è necessario definire la nuova tabella estensioni e i relativi attributi utilizzando Progettazione schema di Web Screen Painter e creare inoltre i moduli necessari per la visualizzazione e l'aggiornamento. Per ulteriori informazioni, vedere Creazione di una nuova struttura di attributi (a pagina 696).

Importante: per estendere CA CMDB è necessario disporre di un'ottima conoscenza delle strutture e delle tabelle di dati di CA SDM, oltre ad avere familiarità con Web Screen Painter (WSP). Si consiglia di contattare i servizi CA per ricevere assistenza in questa attività e di leggere e comprendere a fondo le seguenti sezioni prima di provare a estendere le famiglie e gli attributi di CA CMDB.

Aggiunta di nuovi attributi di CA CMDB

Occorre pianificare con attenzione l'aggiunta di un nuovo attributo di CA CMDB. CA CMDB fornisce molti attributi nelle famiglie e nelle classi predefinite, quindi occorre stabilire se sono adatti alle proprie esigenze prima di iniziare il processo di personalizzazione.

Se si ritiene che è necessario creare un nuovo attributo, si consiglia fare comunque attenzione e porsi le seguenti domande:

- Occorre aggiungere uno o più nuovi attributi a una famiglia esistente?
- Occorre aggiungere i nuovi attributi a più famiglie?

- Occorre aggiungere un nuovo attributo comune, valido per tutte le famiglie?

È possibile estendere una famiglia esistente aggiungendo nuovi attributi. Ad esempio, se ai dispositivi di un'università sono assegnate coordinate GPS, è possibile aggiungere un attributo gps_coordinate a qualsiasi famiglia di elementi della configurazione adeguata. Per ulteriori informazioni, vedere Aggiunta di attributi delle famiglie (a pagina 693).

Dopo aver identificato le esigenze legate agli attributi e se si ritiene di dover utilizzare nuove famiglie e classi, vedere Aggiunta di una nuova famiglia o classe di CA CMDB (a pagina 694).

Aggiunta di attributi delle famiglie

È possibile aggiungere un nuovo attributo a una o più famiglie esistenti con Progettazione schema di Web Screen Painter, che consente di aggiornare il database per includervi il nuovo attributo e aggiornare inoltre le tabelle e i file CA SDM associati. Questo metodo è preferibile rispetto all'aggiornamento manuale delle tabelle e dei file.

Per aggiungere un nuovo attributo a una famiglia

1. Mediante Progettazione schema di Web Screen Painter, aprire lo schema che corrisponde alla tabella estensioni della famiglia.
2. Aggiungere l'attributo desiderato alla tabella estensioni.
3. Pubblicare la tabella estensioni modificata.

Nota: GRLoader e il servizio Controllo delle versioni acquisiscono automaticamente i nuovi attributi senza ulteriori azioni. Tuttavia, si consiglia di attivare la registrazione. La registrazione è richiesta ai fini delle attività di controllo, mentre il servizio Controllo delle versioni è attivato per registrare tutte le snapshot.

Per attivare la registrazione, verificare che UI_INFO per l'attributo sia impostato su **AUDITLOG**.

Dopo aver creato un nuovo attributo per la famiglia, occorre aggiungerlo a ogni modulo di visualizzazione, in modo che gli utenti possano vederlo e aggiornarlo, e anche al modulo di metadati specifico della tabella estensioni. Per ulteriori informazioni, vedere Aggiunta di attributi ai moduli (a pagina 699).

Inoltre, il servizio Controllo delle versioni richiede alcuni metadati, comprese le informazioni sulle intestazioni colonna e i relativi attributi di elementi della configurazione standard. È necessario definire nuovi metadati per tutti i nuovi attributi che si desidera creare; per istruzioni, vedere Creazione dei metadati (a pagina 700).

Aggiunta di attributi comuni

Gli attributi comuni sono memorizzati nella tabella **ca_owned_resource** dell'oggetto **nr**. Questa tabella contiene i seguenti campi personalizzabili:

- smag_1
- smag_2
- smag_3
- smag_4
- smag_5
- smag_6

Se occorrono meno di sette attributi personalizzati in tutte le famiglie di elementi della configurazione, questi campi offrono una soluzione conveniente.

Inizialmente questi campi personalizzati non sono visualizzati in alcun modulo. Per far sì che gli utenti di CA CMDB possano visualizzare o aggiornare un campo smag_*n*, utilizzare Web Screen Painter (Screen Painter Web) e aggiungerlo a qualsiasi modulo visualizzato secondo le proprie esigenze. Tutte le funzioni di registrazione e per GRLoader sono già attivate.

Nota: per le procedure di Progettazione schema di Web Screen Painter, consultare il capitolo "Personalizzazione" della *Guida all'implementazione di CA Service Desk* e la sezione Personalizzazione dello schema del database nella Guida in linea di Web Screen Painter.

Aggiunta di una nuova famiglia o classe di CA CMDB

Occorre pianificare con attenzione l'aggiunta di una nuova famiglia di CA CMDB. CA CMDB fornisce molte famiglie e classi predefinite, quindi occorre stabilire se sono adatte alle proprie esigenze prima di iniziare il processo di personalizzazione. Qualora così non fosse, è possibile far fronte alle nuove esigenze nei seguenti modi:

- definire una nuova classe in una famiglia esistente
- definire una nuova famiglia che utilizza una tabella estensioni esistente

Se si ritiene che le tabelle estensioni esistenti non siano sufficienti per le proprie esigenze, saltare questa sezione e passare alla sezione Creazione di una nuova struttura di attributi (a pagina 696) per creare una tabella estensioni e i moduli richiesti.

Definizione di una nuova classe di elementi della configurazione

È possibile aggiungere di nuove classi per avere una migliore granularità di classificazione. Ad esempio, anziché utilizzare una delle classi fornite da CA CMDB nella famiglia Hardware.Server, è possibile definire classi aggiuntive per dispositivi server diversi.

Prima di creare una classe di un elemento della configurazione, è necessario verificare se nell'elenco delle classi dell'elemento della configurazione esiste già una classe adeguata.

Nota: se è necessaria anche una nuova famiglia per gestire un nuovo gruppo di classi, ignorare questo argomento e passare alla sezione Definizione di una nuova famiglia di elementi della configurazione (a pagina 695). In un secondo momento sarà possibile inserire le classi nella nuova famiglia.

Per definire una classe di elementi della configurazione utilizzando l'interfaccia di amministrazione

1. Accedere all'Elenco classi elementi della configurazione.
2. Fare clic su Crea Nuovo.

   Viene visualizzata la pagina per la creazione di nuova classe elemento della configurazione.
3. Immettere un nome univoco per la nuova classe.
4. Immettere il nome appropriato della famiglia nel campo Famiglia o fare clic sull'icona sopra il campo per cercare una famiglia.
5. Verificare che il campo Stato record sia impostato su Attivo.
6. Fare clic su Salva.

   La nuova classe di elementi della configurazione è definita ed è possibile creare nuovi elementi della configurazione.

Definizione di una nuova famiglia di elementi della configurazione

Prima di creare una famiglia di elementi della configurazione, verificare se esiste già una famiglia appropriata nell'Elenco famiglie elementi della configurazione. In caso contrario, è possibile creare nuove famiglie come metodo alternativo per organizzare o classificare gli elementi della configurazione utilizzando attributi esistenti.

Se la nuova famiglia non può utilizzare una tabella estensioni esistente o quella predefinita, eseguire tutte le operazioni di preparazione delineate in Creazione di una nuova struttura di attributi (a pagina 696). La nuova tabella estensioni può essere utilizzata per definire le nuove famiglie.

Per definire una famiglia di elementi della configurazione utilizzando l'interfaccia di amministrazione

1. Accedere all'Elenco famiglie di elementi della configurazione.
2. Fare clic su Crea Nuovo.

   Viene visualizzata la pagina per la creazione di nuova famiglia elemento della configurazione.
3. Immettere un nome univoco per la nuova famiglia.
4. Verificare che il campo Stato record sia impostato su Attivo.
5. Nel campo Nome estensione, selezionare la tabella estensioni che identifica il tipo di famiglia da creare. Potrebbe trattarsi di una nuova tabella estensioni creata recentemente.

   Se, ad esempio, si sta aggiungendo una famiglia per un tipo di hardware non specificato, selezionare ci_hardware_other. Ciò garantisce che quando si creano nuovi elementi di configurazione le cui classi utilizzano la nuova famiglia, vengano visualizzati gli attributi appropriati nella scheda Attributi. Se non si seleziona un nome tabella nel campo Nome estensione, quando si crea un elemento della configurazione all'interno della nuova famiglia viene utilizzata la tabella predefinita e vengono visualizzati solo gli attributi predefiniti.
6. Immettere una descrizione nel campo Descrizione.

   La descrizione immessa viene visualizzata nell'Elenco famiglie elementi della configurazione a scopo informativo.
7. Fare clic su Salva.

   La famiglia di elementi della configurazione è stata definita.

Una volta definita la nuova famiglia, è possibile aggiungervi classi come descritto in Definizione di una nuova classe di elementi della configurazione (a pagina 695).

Creazione di una nuova struttura di attributi

Se nessuna struttura esistente di classi o famiglie soddisfa le proprie esigenze, è possibile crearne di nuove utilizzando un numero ridotto di attributi. Ciò richiede la creazione di una nuova tabella estensioni e di altre strutture di supporto.

Prima di utilizzare l'interfaccia di amministrazione di CA CMDB per definire una nuova famiglia di elementi della configurazione basata su una nuova tabella estensioni, utilizzare Progettazione schema di Web Screen Painter per creare la nuova tabella estensioni.

Per utilizzare la nuova tabella estensioni, occorre anche creare nuovi moduli HTMPL per:

- la nuova pagina Dettagli elementi della configurazione
- la nuova scheda Attributi con gli attributi associati
- i nuovi moduli di metadati e i metadati

CA CMDB fornisce diversi modelli utili per creare i moduli HTMPL. Le sezioni seguenti forniscono informazioni più dettagliate sulle operazioni da eseguire.

Nota: per le procedure di Progettazione schema di Web Screen Painter, consultare il capitolo "Personalizzazione" della *Guida all'implementazione di CA Service Desk* e la sezione Personalizzazione dello schema del database nella Guida in linea di Web Screen Painter.

Per utilizzare la nuova struttura nell'interfaccia utente di CA CMDB, definire quanto segue:

- una o più famiglie di elementi della configurazione che utilizzano la nuova tabella estensioni
- classi di elementi della configurazione da classificare in base al tipo

Ulteriori informazioni:

Aggiunta di una nuova famiglia o classe di CA CMDB (a pagina 694)

Creazione di una nuova tabella estensioni

Prima di definire una famiglia basata su una nuova tabella estensioni, occorre aggiornare il database con la nuova tabella e aggiornare anche lo schema CA CMDB con le informazioni relative alla tabella.

Per creare una tabella estensioni

1. Mediante Progettazione schema di Web Screen Painter, definire la nuova tabella estensioni e un nome estensione.
2. Salvare e pubblicare la nuova tabella estensioni.

Nota: Progettazione schema di Screen Painter Web crea automaticamente il trigger di registrazione in CA CMDB.

Andare alla sezione successiva per creare la pagina Dettagli elementi della configurazione.

Creazione di una pagina Dettagli elementi della configurazione

È richiesta una pagina Dettagli elementi della configurazione per supportare la visualizzazione degli attributi per gli elementi della configurazione associati a una nuova tabella estensioni.

Per creare la pagina Dettagli degli elementi della configurazione

1. Mediante Progettazione schema di Web Screen Painter, fare clic su File, Nuovo e creare un modulo basato su detail_extension.template.
2. Salvare questo nuovo modulo come **detail_*extension*.htmpl**, dove *extension* è il nome della tabella estensioni.
3. Seguire le istruzioni elencate nel file, sostituendo la stringa ***EXTENSION*** con il nome della nuova tabella estensioni (definito precedentemente).
4. Salvare il file con tutte le modifiche.

La pagina Dettagli elementi della configurazione contiene due sezioni per gli attributi:

- la sezione degli attributi comuni denominata cmdb_detail.htmpl
- la sezione specifica per la famiglia (scheda Attributi) denominata nr_cmdb_extension_tab.htmpl, dove *extension* è il nome della nuova tabella estensioni.

Andare alla sezione successiva per creare la scheda Attributi elementi della configurazione (a pagina 698).

Creazione di una scheda Attributi elementi della configurazione

La scheda Attributi visualizza gli attributi specifici della famiglia per un elemento della configurazione.

Per creare la scheda Attributi

1. Mediante l'editor visivo di Web Screen Painter, fare clic su File, Nuovo e creare un modulo basato su nr_cmdb_extension_tab.template.
2. Salvare questo file come **nr_cmdb_*extension*_tab.htmpl**, dove *extension* è il nome della nuova tabella estensioni.
3. Seguire le istruzioni elencate nel file, sostituendo la stringa ***EXTENSION*** con il nome della nuova tabella estensioni (definito precedentemente).
4. Salvare e pubblicare il file con tutte le modifiche.

Andare alla sezione successiva per inserire i dati nella scheda Attributi.

Aggiunta di attributi ai moduli

Dopo aver utilizzato Progettazione schema di Web Screen Painter per creare un nuovo attributo in una tabella estensioni, l'attributo deve essere aggiunto a un modulo utilizzato per la visualizzazione o l'aggiornamento. Per i nuovi attributi specifici delle famiglie, l'unico modulo che occorre modificare è la scheda Attributi denominata **nr_cmdb_***extension***_tab.htmpl**, dove *extension* è il nome della tabella estensioni. Questo modulo deve essere modificato in modo da contenere qualsiasi nuovo attributo.

Per modificare un modulo di attributi

1. Mediante l'editor visivo di Web Screen Painter, fare clic su File, Apri per accedere al modulo appropriato.
2. Trascinare i nuovi attributi nel modulo.

   Nota: i moduli forniti da CA CMDB non possono essere modificati con l'editor visivo di Web Screen Painter, quindi occorre utilizzare l'editor di testo di Web Screen Painter nella scheda Progetto.

3. Salvare e pubblicare il modulo.

Se non è stato ancora creato un modulo di metadati, vedere la sezione Creazione di un modulo di metadati (a pagina 699). Per definire i metadati di un nuovo attributo nel modulo, vedere la sezione Creazione dei metadati (a pagina 700).

Creazione di un modulo di metadati

Una nuova tabella estensioni richiede un proprio modulo di metadati per definire le intestazioni colonna e le informazioni degli elementi della configurazione standard per il servizio Controllo delle versioni.

Per creare il modulo di metadati

1. Mediante l'editor visivo di Web Screen Painter, fare clic su File, Apri per accedere a cmdb_metadata_extension.template.
2. Salvare questo file come **cmdb_metadata_***extension***.htmpl**, dove *extension* è il nome della tabella estensioni.
3. Seguire le istruzioni elencate nel file, sostituendo la stringa ***EXTENSION*** con il nome della nuova tabella estensioni (definito precedentemente).
4. Salvare e pubblicare il modulo con tutte le modifiche.

Andare alla sezione successiva per inserire i dati nel modulo dei metadati.

Creazione dei metadati

I metadati contengono informazioni sulle intestazioni colonna degli attributi e sugli elementi della configurazione standard richiesti dalla funzione Controllo delle versioni.

Importante: occorre pianificare con attenzione i metadati per fare in modo che le snapshot contengano i dati corretti, la funzione Controllo delle versioni contenga i titoli corretti e i confronti degli elementi della configurazione standard riescano.

Per creare metadati

1. Utilizzare l'editor visivo di Web Screen Painter, fare clic su File, Apri per accedere a **cmdb_metadata_***extension***.htmpl**, dove *extension* è il nome della tabella estensioni.
2. Seguendo le istruzioni elencate nel modulo, copiare e modificare la riga indicata per ogni attributo nella nuova tabella estensioni.

   Nota: gli attributi seguenti, sebbene obbligatori, non richiedono metadati:

   - ID
   - Last_modified_by
   - Etc (da specificare)
3. Salvare e pubblicare tutte le modifiche.

Se si aggiungono metadati a una famiglia CA CMDB esistente, le modifiche di audit saranno visualizzate correttamente nella scheda Controllo delle versioni. Tuttavia, se si definiscono metadati per una nuova tabella estensioni, occorre disporre di una nuova famiglia e di una nuova classe per gli attributi; per ulteriori informazioni, vedere Aggiunta di una nuova famiglia o classe di CA CMDB (a pagina 694).

Ora sono disponibili le strutture per la nuova tabella estensioni. Per definire una nuova famiglia per gli attributi, vedere Definizione di una nuova famiglia di elementi della configurazione (a pagina 695).

Esempio

In questo esempio, vengono create una famiglia **Automobili** e una classe **Berlina** al suo interno per tenere traccia delle risorse di inventario per produzione, spedizione, noleggio o gli altri scopi. Ovviamente è possibile creare molte altre classi di automobili; questo esempio è puramente dimostrativo.

Passaggio 1: Creazione della nuova tabella estensioni

1. In Progettazione schema di Web Screen Painter, fare clic su Aggiungi tabella estensioni.
2. Immettere un nome per la nuova tabella estensioni. In questo esempio, **veicolo**.

   La tabella estensioni **zveicolo** viene creata e le sue proprietà sono visualizzate.

   Nota: la lettera "z" viene aggiunta all'inizio di tutti i nomi delle nuove tabelle per distinguerle da quelle fornite dall'applicazione.
3. Nella scheda Informazioni tabella, impostare il campo Gruppo funzioni su **inventory**. Negli altri campi vengono inseriti i valori predefiniti.
4. Aggiungere nuove colonne e informazioni sugli attributi come desiderato.
5. Salvare e pubblicare la nuova tabella estensioni.

Passaggio 2: Creazione di una nuova famiglia

Per creare una famiglia

1. Accedere all'Elenco famiglie elementi della configurazione.
2. Fare clic su Crea nuovo.

   Viene visualizzata la pagina Crea nuova famiglia elementi della configurazione.
3. Immettere un nome univoco per la nuova famiglia. In questo esempio, **Automobili**.
4. Verificare che il campo Stato record sia impostato su Attivo.
5. Selezionare il nome della tabella estensioni. In questo esempio, **zveicolo**.
6. Fare clic su Salva.

   La nuova famiglia di elementi della configurazione è stata creata.

Passaggio 3: Creazione di una nuova classe

1. Accedere all'Elenco classi elementi della configurazione.
2. Fare clic su Crea nuovo.

   Viene visualizzata la pagina Crea nuova classe elementi della configurazione.
3. Immettere un nome univoco per la nuova classe. In questo esempio, **Berlina**
4. Verificare che il campo Stato record sia impostato su Attivo.
5. Selezionare la famiglia. In questo esempio, **Automobili**.
6. Fare clic su Salva.

   La nuova classe di elementi della configurazione è stata creata.

Passaggio 4: Creazione del nuovo modulo Dettagli elementi della configurazione

Per creare il modulo Dettagli degli elementi della configurazione

1. Nell'editor visivo di Web Screen Painter, aprire il modulo detail_extension.template.
2. Salvare il modello con il nome **detail_zveicolo.htmpl**.

   Il nuovo modulo viene salvato in NX_ROOT\site\mods\wsp\project\web\analyst
3. Nel nuovo modulo, sostituire tutte le istanze di ***EXTENSION*** con **zveicolo.**
4. Salvare e pubblicare il nuovo modulo Dettagli elementi della configurazione.

Passaggio 5: Creazione della scheda Attributi

Per creare il modulo della scheda Attributi

1. Nell'editor visivo di Web Screen Painter, aprire il modulo nr_cmdb_extension_tab.template.
2. Salvare il modello con il nome **nr_cmdb_zveicolo_tab.htmpl**.

   Il nuovo modulo viene salvato in NX_ROOT\site\mods\wsp\project\web\analyst
3. Nel nuovo modulo, sostituire tutte le istanze di ***EXTENSION*** con **zveicolo.**
4. Aggiungere gli attributi al modulo come desiderato.
5. Salvare e pubblicare il nuovo modulo della scheda Attributi.

Passaggio 6: Creazione del modulo di metadati

Per creare il modulo di metadati

1. Nell'editor visivo di Web Screen Painter, aprire il modulo cmdb_metadata_extension.template
2. Salvare il modello con il nome **cmdb_metadata_zveicolo.htmpl**

   Il nuovo modulo viene salvato in NX_ROOT\site\mods\wsp\project\web\analyst
3. Sostituire tutte le occorrenze ***EXTENSION*** con **zveicolo.**
4. Mediante i segnaposti per intestazioni e attributi, aggiungere i metadati per tutti gli attributi specifici della famiglia.
5. Salvare e pubblicare il nuovo modulo di metadati.

Funzionalità CACF (Configuration Audit and Control Facility)

La funzionalità CACF (Configuration Audit and Control Facility) unifica tre discipline, ovvero Gestione Cambiamento, Gestione della configurazione (CMDB) e Gestione del rilevamento per verificare che i cambiamenti vengano eseguiti in modo accurato e che non si verifichi alcun cambiamento non autorizzato.

La Verifica del Cambiamento aiuta a garantire che CMDB rifletta tutti i cambiamenti in modo accurato e che gli strumenti di Gestione del rilevamento verifichino i cambiamenti.

La Verifica del Cambiamento apporta i seguenti vantaggi:

Gestione dei Cambiamenti

- Garanzia che i cambiamenti autorizzati vengano eseguiti correttamente
- Rilevamento di Cambiamenti eseguiti in modo incorretto
- Rilevamento dei cambiamenti non autorizzati
- Reporting di gestione
- Controllo completo di tutti i cambiamenti nel livello di attributo
- Rilevamento dei cambiamenti sovrapposti o in conflitto

Gestione della configurazione

- CMDB contiene una rappresentazione accurata e attuale di tutti gli elementi della configurazione gestiti
- Visualizzazione dello stato futuro degli elementi della configurazione con le specifiche di Cambiamento suggerite
- Controllo completo degli elementi della configurazione

La funzionalità CACF ha due sezioni principali, l'interfaccia amministrativa di CMDB e l'interfaccia di gestione dei Cambiamenti (illustrata in modo dettagliato nelle sezioni a seguire).

Ulteriori informazioni:

Amministrazione della funzionalità CACF e definizione delle policy (a pagina 705)
Attributi gestiti (a pagina 721)
Stati del Cambiamento gestito (a pagina 722)
Specifiche del Cambiamento (a pagina 724)
Modalità di funzionamento della verifica del Cambiamento (a pagina 730)
Archiviazione ed eliminazione dei dati di audit (a pagina 736)
Implementazione della strategia di verifica del Cambiamento. (a pagina 737)
Progettazione e implementazione della verifica di Cambiamento. (a pagina 742)
Procedure consigliate di verifica dei Cambiamenti (a pagina 749)
Verifica manuale di aggiornamento del valore dell'attributo dell'elemento della configurazione (a pagina 753)
Esempio: Autorizzazione degli aggiornamenti non autorizzati solo da una posizione specifica (a pagina 758)
Esempio: Aggiornamento dei computer portatili dell'organizzazione (a pagina 760)
Esempio: Blocco degli Ordini di cambiamento non verificati (a pagina 761)
Esempio: Autorizzazione dell'aggiornamento dell'elemento della configurazione nel caso in cui non esista un Ordine di cambiamento corrispondente (a pagina 762)
Esempio: Rinvio degli aggiornamenti da CA Configuration Automation all'area di lavoro della transazione (a pagina 762)
Esempio: Registrazione dei risultati della policy come test (a pagina 763)
Esempio: Rifiuto dell'aggiornamento di un elemento della configurazione (a pagina 763)
Esempio: Autorizzazione di Ordini di cambiamento creati senza specifiche (a pagina 764)
Esempio: Blocco dell'autorizzazione di Ordini di cambiamento creati senza specifiche (a pagina 764)
Esempio: Autorizzazione degli inserimenti non autorizzati da origini selezionate (a pagina 765)
Esempio: Autorizzazione di un aggiornamento non autorizzato per un elemento della configurazione non appartenente alla produzione (a pagina 765)

Amministrazione della funzionalità CACF e definizione delle policy

L'amministratore CMDB definisce gli elementi della configurazione e gli attributi gestiti, nonché la policy di aggiornamento per tali elementi della configurazione e attributi. I componenti CACF vengono amministrati a partire dal nodo Controllo della configurazione nella sezione CA CMDB della scheda Amministrazione e consentono di definire e visualizzare le specifiche di Cambiamento CACF da moduli Ordine di Cambiamento, Elemento della configurazione e Incidente o dal nodo Audit della configurazione nella scheda Amministrazione.

L'amministratore deve considerare di autorizzare le modifiche standard, definire le origini dati autorevoli e attendibili, oltre a definire gli elementi della configurazione e i relativi attributi da includere nella gestione CACF. In caso di esecuzione incorretta o non autorizzata di un Cambiamento (nota anche come varianza), CA SDM può accettare il nuovo valore, creare un Incidente, oppure copiare i dati all'area di lavoro transazione per elaborarli in un secondo momento. CA SDM può utilizzare qualsiasi combinazione di queste azioni.

Importante: Gli amministratori della configurazione *devono* stabilire una strategia di verifica del Cambiamento (a pagina 737) per l'ambiente dell'utente. La policy predefinita per CACF autorizza tutti i Cambiamenti agli elementi della configurazione, inclusi i Cambiamenti non autorizzati o non corrispondenti ad un ticket di Cambiamento.

È possibile implementare policy di verifica dei Cambiamenti in modo dinamico o pianificato È possibile definire queste policy come generiche o estremamente specifiche. La policy di verifica del Cambiamento descrive il comportamento di risposta di CA SDM ai seguenti eventi:

Aggiornamenti da MDR non autorizzati

Indica che MDR specifici sono autorizzati per determinati attributi. È possibile accettare o rifiutare in modo selettivo gli aggiornamenti dell'attributo dell'elemento della configurazione eseguiti da MDR non autorizzati.

Ad esempio, definire policy per impedire a CA Application Configuration Manager di aggiornare l'indirizzo IP di un elemento della configurazione, anche nel caso in cui sia presente un Ordine di Cambiamento corrispondente. Consentire gli aggiornamenti dell'indirizzo IP soltanto nel caso in cui l'MDR di origine corrisponda a Spectrum.

Cambiamenti non autorizzati

Rileva e gestisce gli aggiornamenti degli elementi della configurazione quando non è presente un Ordine di Cambiamento corrispondente. È possibile specificare una policy per la gestione dei Cambiamenti non autorizzati che richiedono l'inserimento o l'aggiornamento dei dati dell'elemento della configurazione.

Ad esempio, quando un elemento della configurazione denominato server* a New York viene modificato ma non dispone di un Ordine di Cambiamento corrispondente, sarà necessario caricare i dati dell'area di lavoro della transazione invece di eseguire l'aggiornamento dell'elemento della configurazione.

Cambiamenti eseguiti con errori

Individua quando un Ordine di Cambiamento non viene implementato (a pagina 708) correttamente.

Le funzionalità di audit consentono al manager della configurazione di visualizzare le modifiche apportate alle policy e le definizioni di oggetto CACF. CACF registra ciascun tentativo di aggiornamento dell'elemento della configurazione, a prescindere se l'aggiornamento era autorizzato. Il registro consente di stabilire quale policy ha autorizzato o negato un Cambiamento all'elemento della configurazione.

L'amministratore della configurazione definisce quali stati dell'Ordine di Cambiamento sono modificabili e quali rappresentano stati di verifica. Per impostazione predefinita, è possibile modificare specifiche del Cambiamento quando lo stato dell'Ordine di Cambiamento corrisponde a *RFC* mentre la verifica del Cambiamento si produce quando un Ordine di Cambiamento è in stato *Verifica in corso*. Facoltativamente, è inoltre possibile promuovere o chiudere i ticket di Cambiamento in modo automatico se tutte le specifiche di Cambiamento associate vengono eseguite correttamente.

Importante: Quando viene abilitata l'opzione Crea Incidente con più di una policy di verifica attiva, potrebbe verificarsi una diminuzione delle prestazioni.

Nota: Per impostazione predefinita, CACF considera gli aggiornamenti dei valori di attributo per gli Ordini di Cambiamento con la verifica dei cambiamenti attiva quando modifiche autorizzate vengono applicate nella Verifica in corso. L'amministratore della configurazione può modificare tale comportamento (a pagina 722).

Ulteriori informazioni:

Definizione delle specifiche del Cambiamento da parte degli analisti del Cambiamento (a pagina 707)
Verifica del Cambiamento (a pagina 708)
Modalità di utilizzo delle specifiche di Cambiamento da parte dei manager del Cambiamento. (a pagina 709)
Modalità di funzionamento della funzionalità CACF (a pagina 710)

Definizione delle specifiche del Cambiamento da parte degli analisti del Cambiamento

La porzione dell'interfaccia di gestione del Cambiamento della verifica del Cambiamento viene integrata nel modulo del ticket dell'Ordine di Cambiamento. Gli analisti del Cambiamento creano le specifiche del Cambiamento al momento della creazione dell'Ordine di Cambiamento. Inoltre, definiscono il Cambiamento a seconda dell'elemento della configurazione e del relativo attributo che desiderano modificare.

Per includere una descrizione della specifica del Cambiamento, gli analisti possono utilizzare uno dei seguenti modelli:

- Specificare il nome esatto, l'attributo e il valore dell'elemento della configurazione.

  Ad esempio, dopo l'implementazione del Cambiamento, l'indirizzo IP del server1 viene impostato su 10.10.10.10.

- Specificare l'attributo e il valore dell'elemento della configurazione e omettere il nome dell'elemento della configurazione.

  Ad esempio, dopo il Cambiamento, la memoria di tutti gli elementi della configurazione associati all'Ordine di Cambiamento viene aggiornata a 8GB.

- Fornire un valore di attributo da impostare quando l'attributo non è rilevabile.

  Ad esempio, dopo il Cambiamento, CMDB indica NY come posizione di tutti gli elementi della configurazione.

- Utilizzare il valore rilevato.

  Ad esempio, prima del Cambiamento non è possibile stabilire quale sarà il nuovo indirizzo IP, ma si sa con certezza che l'indirizzo IP verrà modificato. Impostare l'indirizzo IP dell'elemento della configurazione su qualsiasi valore rilevato dall'MDR autorizzato.

Quando l'Ordine di Cambiamento viene approvato, le specifiche del Cambiamento vengono approvate come parte dello stesso processo di approvazione. Successive modifiche delle specifiche possono essere impedite e vengono totalmente controllate.

Verifica del Cambiamento

La Verifica del Cambiamento consente di garantire che gli Ordini di Cambiamento rispettino le specifiche di Cambiamento. La verifica avviene dopo che un Ordine di Cambiamento entra in uno stato di gestione Cambiamento, come lo stato Verifica in corso, e quando si verifica un qualunque tipo di aggiornamento dell'elemento della configurazione. A tal punto, quando i dati di un MDR o utente del client Web vengono importati in CMDB, la funzionalità CACF compara i dati dell'attributo in entrata con le specifiche di Cambiamento attive. Se i dati dell'attributo dell'elemento della configurazione coincidono, la funzionalità CACF verifica il Cambiamento. Se i dati in entrata non corrispondono alle specifiche dell'Ordine di Cambiamento, le azioni per rimediare la varianza dipenderanno dalla policy.

Le policy possono effettuare tutte le seguenti azioni:

- Rifiutare l'aggiornamento di un determinato attributo dalla transazione.
- Rifiutare l'intera transazione, incluse tutte le coppie attributo-valore.
- Caricare l'intera transazione nell'area di lavoro transazione per l'elaborazione differita a seguito dell'approvazione e verifica della transazione.
- Creare un Incidente che descrive ciascuna varianza.

  Nota: questa azione può attivare le notifiche e le automazioni esistenti. Per impedire la creazione di Incidenti multipli, il rilevamento di Cambiamenti non autorizzati crea un singolo Incidente per tutti i Cambiamenti non autorizzati di un elemento della configurazione.

- Accettare la transazione incondizionatamente al momento dell'accettazione dei dati dagli MDR di origine autorizzati.

Ad esempio, l'amministratore di CMDB può definire una policy in grado di creare un Incidente quando si verifica un errore di esecuzione di modifica di un server di produzione. Quando i dati importati da un MDR autorizzato non corrispondono a una specifica di un Cambiamento in sospeso, la funzionalità CACF crea un Incidente. Il criterio può consentire o respingere un aggiornamento dell'elemento della configurazione in base ai dati di importazione non corrispondenti. Inoltre, la Gestione Cambiamento può accettare il nuovo valore rilevato, anche se tale valore non corrisponde esattamente alla specifica di Cambiamento pianificata.

Nota: Qualora si verificassero rilevamenti multipli durante la verifica della specifica di Cambiamento, i dati rilevati potranno invalidare una modifica precedentemente verificata. Al termine della verifica, lo stato dell'elemento della configurazione corrisponde allo stato richiesto per tutte le specifiche del Cambiamento.

Modalità di utilizzo delle specifiche di Cambiamento da parte dei manager del Cambiamento.

Il manager del Cambiamento effettua le seguenti operazioni:

- Visualizzazione e modifica dello stato di verifica di tutte le specifiche del Cambiamento.

  Ad esempio, il manager del Cambiamento desidera sapere quali specifiche sono ancora in sospeso per l'Ordine di Cambiamento 12345 con stato *In attesa di verifica.*

- Gestione degli Incidenti per i Cambiamenti non autorizzati o eseguiti incorrettamente.

  Ad esempio, il manager del Cambiamento desidera visualizzare i Cambiamenti con verifica non riuscita e quelli che necessitano di ulteriori ricerche.

- Gestione dei Cambiamenti che richiedono intervento manuale.

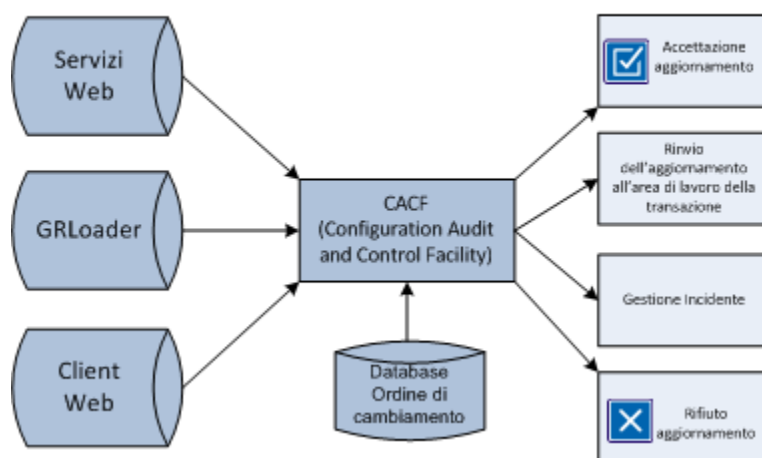
  Ad esempio, un Ordine di Cambiamento richiede la verifica manuale per un Cambiamento non rilevabile e l'analista del Cambiamento deve completare l'attività.

  Ad esempio, il manager del Cambiamento indaga e determina che l'Ordine di Cambiamento 12345 identifica dieci specifiche di Cambiamento differenti. A causa di un errore di battitura, la specifica di Cambiamento numero 9 era erronea, quindi eliminabile.

Le funzionalità di controllo forniscono la possibilità di visualizzare lo stato di ciascun aggiornamento della specifica di Cambiamento nonché qualsiasi sostituzione di tale specifica. Il contatore mostra lo stato del sistema in esecuzione ed eventuali condizioni particolari che richiedono intervento o analisi. I rapporti di CA Business Intelligence forniscono una visione a lungo termine dell'efficienza delle policy di Gestione configurazione per il controllo dello stato dell'ambiente dell'utente.

Modalità di funzionamento della funzionalità CACF

La funzionalità CACF regola i dati in entrata dell'elemento della configurazione prima del caricamento in CMDB. Tale verifica consente di garantire che tutti gli Ordini di Cambiamento necessari vengano eseguiti correttamente. Inoltre, individua e gestisce automaticamente le modifiche non autorizzate. L'amministratore della configurazione (l'amministratore di CMDB) definisce policy di verifica per determinare le modalità di risposta di CA SDM in caso di deviazione o varianza dal Cambiamento richiesto.

Il diagramma seguente mostra la modalità di funzionamento della funzionalità CACF:

1. I dati in entrata dell'elemento della configurazione vengono caricati dai servizi Web, GRLoader, MDR o dall'Interfaccia Web per richiedere l'aggiornamento attributo di un elemento della configurazione in CMDB.
2. In base alle policy di verifica stabilite dall'amministratore della configurazione, la funzionalità CACF completa una o di più delle seguenti azioni:
   - Accetta l'aggiornamento e modifica i dati dell'elemento della configurazione in CMDB.
   - Rinvia l'elaborazione dell'aggiornamento all'area di lavoro transazione.

     Ad esempio, il manager del Cambiamento gestisce le transazioni dell'area di lavoro transazione.
   - Crea un Incidente e lascia all'utente la gestione del ticket.

     Ad esempio, il processo di gestione Incidente dell'utente richiede la gestione dell'Incidente a fini di reporting.
   - Respinge l'aggiornamento e i dati dell'elemento della configurazione non vengono modificati nel database.

Policy di verifica

Quando il manager della configurazione e il manager del Cambiamento concordano su una policy di verifica del Cambiamento, le loro decisioni vengono trascritte in una policy di verifica del Cambiamento di CA SDM. Un sistema può disporre di più policy di verifica. Quando si verifica l'aggiornamento di un elemento della configurazione, la funzionalità CACF seleziona un'unica policy di verifica per ciascun attributo aggiornato. Tale policy sarà in grado di decidere dell'aggiornamento dell'elemento della configurazione nonché dell'eventuale creazione di una voce dell'area di lavoro transazione o di un Incidente relativo all'esistenza di una specifica di Cambiamento corrispondente.

Nota: se si desidera monitorare gli aggiornamenti mediante il client Web, specificare il modello della classe MDR come **client Web** (distinzione maiuscole/minuscole) nella policy di verifica. Questo modello viene applicato alle versioni in lingua inglese e localizzate di CA SDM quando si desidera monitorare gli aggiornamenti mediante il client Web.

Importante Per determinare le policy più adatte al proprio ambiente, è necessaria una valutazione approfondita degli obiettivi della propria organizzazione e delle modalità con cui si desidera introdurre tali policy.

Selezione di una policy di verifica

Quando si verifica l'aggiornamento di un elemento della configurazione, la funzionalità CACF seleziona una policy per ciascun attributo aggiornato. Tale selezione dipende dall'origine dell'aggiornamento, dall'elemento della configurazione di destinazione e dall'eventuale esistenza di una specifica di Cambiamento corrispondente. Quando varie policy coincidono, la funzionalità CACF seleziona la policy con il più basso numero di sequenza per gestire l'aggiornamento dell'attributo.

Nota: la funzionalità CACF può selezionare più policy per gestire una transazione singola in grado di aggiornare attributi multipli. Ad esempio, l'aggiornamento di un elemento della configurazione con una nuova descrizione e un nuovo indirizzo IP può attivare due policy differenti.

Ciascuna policy dispone di quattro sezioni che CACF utilizza nella selezione della policy:

Identificazione e priorità

Identifica una policy e ne specifica l'ordine di valutazione.

Allineamento dell'Ordine di Cambiamento

Seleziona le transazioni in base alla maggiore o minore corrispondenza dell'aggiornamento attributo con una specifica esistente.

Filtro transazione

Specifica le fonti di dati a cui si applica la policy.

Filtro dell'elemento della configurazione

Specifica gli elementi della configurazione a cui si applica la policy.

Una policy corrisponde ad un aggiornamento attributo quando passa ciascuno di tali filtri. Se una policy non corrisponde ad una transazione, la funzionalità CACF ignora la policy e ne valuta altre presenti nel sistema. Se la funzionalità CACF ignora tutte le policy, per impostazione predefinita viene concesso l'aggiornamento dell'attributo.

Sintassi del filtro della policy di verifica

Per permettere l'elaborazione di policy generiche, l'allineamento dell'Ordine di cambiamento, il filtro transazione e il filtro dell'elemento della configurazione consentono l'uso di un asterisco come carattere finale jolly. Per indicare una negazione, è possibile utilizzare un punto esclamativo all'inizio del filtro.

Importante Le regole del modello di policy sono diverse dalle regole utilizzare per il valore pianificato della specifica del Cambiamento. Per i filtri delle policy, non è possibile utilizzare asterischi (*) segni di maggiore (>) e minore (<) o caratteri speciali.

I filtri delle policy eseguono la distinzione maiuscole/minuscole per i modelli di selezione delle policy di verifica, quali nomi degli elementi della configurazione o classi degli elementi della configurazione, anche se tali attributi vengono definiti senza distinzione maiuscole/minuscole.

Nota: un filtro di policy vuoto "" (senza alcun valore specificato nel campo corrispondente) recupera solo valory vuoti, mentre un filtro di policy che utilizza un asterisco consente di recuperare qualsiasi valore.

Considerare le seguenti informazioni e le relative policy di verifica di esempio:

- Policy1 seleziona gli elementi della configurazione nome(prod*) con attributo(Indirizzo IP) per cui esiste una specifica del Cambiamento corrispondente.
- Policy2 seleziona gli elementi della configurazione nome(prod*) con attributo(Indirizzo IP) per cui è presente un aggiornamento non autorizzato.
- Policy3 seleziona gli elementi della configurazione nome(test*) e attributo(Memoria installata) da mdr(Cohesion).
- Policy4 seleziona gli elementi della configurazione nome(”) con attributo(Memoria installata).

Il seguente elenco descrive i possibili esiti di tali policy:

- Quando si verifica un aggiornamento dell'elemento della configurazione(test2) con attributo(Memoria installata), Policy3 gestisce l'aggiornamento. La funzionalità CACF ignora Policy1 e Policy2.
- Quando si verifica un aggiornamento dell'elemento della configurazione(prod3) con attributo(Memoria installata) ed esiste al contempo una specifica del Cambiamento, Policy1 gestisce l'aggiornamento.
- Quando si verifica un aggiornamento dell'elemento della configurazione(development4) con attributo(Indirizzo IP), la funzionalità CACF aggiorna l'elemento della configurazione con il nuovo indirizzo IP in quanto non esistono policy corrispondenti.
- Quando si verifica un aggiornamento dell'elemento della configurazione(prod1) con attributo(Capacità disco) e non sono presenti policy per l'attributo (Capacità disco), la funzionalità CACF aggiorna l'elemento della configurazione con il nuovo valore. In tale esempio, la funzionalità CACF *non* gestisce l'attributo Capacità disco.
- Policy4 recupera solo gli elementi della configurazione con nomi vuoti. Le modifiche non vengono eseguite, in quanto i nomi vuoti non sono nomi validi.

Assegnazione della priorità della policy di verifica per numero di sequenza

Quando esistono più policy corrispondenti ad un aggiornamento attributo, la funzionalità CACF sceglie la policy con il numero di sequenza inferiore. Considerare le seguenti policy e i loro numeri di sequenza.

- Nome policy(Policy1) sequenza(1000) elemento della configurazione(prod*)
- Nome policy(Policy2) sequenza(2000) elemento della configurazione(prod-NY*)

Quando si verifica un aggiornamento dell'elemento della configurazione(prod1), Policy1 gestisce la transazione. Quando si verifica un aggiornamento dell'elemento della configurazione(prod-NY-1), la transazione continua ad essere gestita da Policy1, in quanto tale policy ha un numero di sequenza più basso. Nell'esempio seguente, Policy2 non interviene mai.

Si consiglia di modificare i numeri di sequenza in modo tale che il criterio più specifico abbia il numero di sequenza più basso, come illustrato nelle seguenti policy di esempio:

- Nome policy(Policy1) sequenza(2000) elemento della configurazione(prod*)
- Nome policy(Policy2) sequenza(1000) elemento della configurazione(prod-NY*)

Quando si verifica un aggiornamento dell'elemento della configurazione(prod1), Policy1 gestisce la transazione. Quando si verifica un aggiornamento dell'elemento della configurazione(prod-NY-1), la transazione continua ad essere gestita da Policy2, in quanto tale policy ha un numero di sequenza più basso.

Allineamento dell'Ordine di Cambiamento

Le policy filtrano in base alla maggiore o minore corrispondenza dell'aggiornamento attributo dell'elemento della configurazione con una specifica di Cambiamento. Dopo un aggiornamento dell'elemento della configurazione, la funzionalità CACF ricerca una specifica di Cambiamento corrispondente al nome dell'elemento della configurazione e dell'attributo. Tale ricerca può verificare la specifica di Cambiamento. L'allineamento dell'Ordine di Cambiamento può verificarsi come segue:

- Esistono specifiche di Cambiamento per l'elemento della configurazione e l'attributo.
- Esistono Ordini di Cambiamento che *non* contengono specifiche di Cambiamento per l'elemento della configurazione.
- Si verifica una transazione di inserimento non autorizzata indicante un nuovo elemento della configurazione e *non* esistono Ordini di Cambiamento con tale elemento della configurazione associato.
- Si verifica una transazione di aggiornamento non autorizzata indicante un elemento della configurazione esistente e non esistono Ordini di Cambiamento con tale elemento della configurazione associato.

Durante la ricerca per corrispondenza di Ordini di Cambiamento, vengono considerati solo gli Ordini di Cambiamento che si trovano in uno stato di modifica in cui la *Verifica di Cambiamento è attiva*. Gli Ordini di Cambiamento chiusi, non approvati, non pianificati o non eseguiti non vengono considerati al momento della ricerca.

Una volta determinato l'allineamento di una transazione dell'Ordine di Cambiamento, la funzionalità CACF cerca di individuare la policy corrispondente. Una policy può gestire uno o più tipi di allineamento di Ordine di Cambiamento:

Ordine di Cambiamento con specifiche

Indica l'esistenza di un Ordine di Cambiamento con una specifica di Cambiamento che identifica un aggiornamento dell'elemento della configurazione e del nome attributo.

Ordini di Cambiamento senza specifiche

Indica Ordini di Cambiamento che specificano l'aggiornamento dell'elemento della configurazione e che non hanno nessuna specifica di Cambiamento.

Inserimento non autorizzato

Indica un elemento della configurazione inserito. Per definizione, l'elemento della configurazione non ha Ordini di Cambiamento in stato di verifica associati.

Importante. Le policy che bloccano inserimenti non autorizzati devono specificare un attributo gestito *Nome* o *Tutti gli attributi gestiti*, in cui *Nome* specifica un attributo gestito attivo.

La funzionalità CACF consente sempre inserimenti e aggiornamenti non autorizzati quando una transazione dispone solo di attributi non gestiti.

Aggiornamento non autorizzato

Indica un elemento della configurazione aggiornato e senza Ordini di Cambiamento associati in stato di verifica.

Ulteriori informazioni:

Esempio: Autorizzazione di Ordini di cambiamento creati senza specifiche (a pagina 764)
Blocco dei Cambiamenti non autorizzati per l'attributo (a pagina 747)

Esempio: Policy di allineamento dell'Ordine di Cambiamento

Le seguenti policy di esempio specificano allineamenti dell'Ordine di Cambiamento:

- Policy name(legacy) filtra CI(*) attribute(Tutti gli attributi gestiti) alignment(Ordini di cambiamento senza specifiche) action(Consenti aggiornamento dell'attributo)
- Policy name(nuovo) filtra CI(*) attribute(Tutti gli attributi gestiti) alignment(Ordini di cambiamento con specifiche) action(Consenti aggiornamento solo in caso di corrispondenza con la specifica del Cambiamento)
- Policy name(diverso da non autorizzato) filtra CI(*) attribute(Tutti gli attributi gestiti) alignment(inserimento non autorizzato o aggiornamento non autorizzato) action(Annulla sempre l'intera transazione, Crea Incidente)

Le funzionalità offerte da tali policy di esempio sono:

- La Policy(legacy) consente agli Ordini di cambiamento di CA SDM r12.6 senza specificazioni di aggiornare l'elemento della configurazione come nell'implementazione CACF.
- Policy(new) impone la verifica del Cambiamento a tutti gli Ordini di cambiamento con specifiche del Cambiamento associate.
- La Policy(no-rogue) non consente gli aggiornamenti dell'elemento della configurazione se non è presente alcun Ordine di cambiamento con stato Verifica del Cambiamento attiva.

Filtro transazione

Le policy filtrano le transazioni in base all'origine della transazione, includendo il nome attributo, il nome MDR, la classe MDR e il ruolo (a pagina 712) dell'utente che esegue l'aggiornamento.

Nota: se si desidera filtrare solo gli utenti connessi all'interfaccia Web, specificare la parola chiave **Web Client** per la classe MDR. L'ID utente del contatto si riferisce al nome dell'MDR. Questo metodo di identificazione degli utenti si applica solo alle policy di verifica e non compare in altre parti del prodotto.

Esempio: Filtri di transazione

Le seguenti policy di esempio specificano filtri di transazione:

- Policy name(accesso_directory_principale) filtra ci(*) attribute(Tutti gli attributi gestiti) role(Amministratore) action(Consenti aggiornamento dell'attributo)
- Policy name (cohesion_non_autorizzato) filtra ci(*) attribute(Indirizzo IP) MDRclass(Cohesion) action(Mantieni il valore di attributo precedente)
- Policy name(john) filtra ci(user1*) attribute(Tutti gli attributi gestiti) MDRName(user1) MDRClass(Client Web) action(Consenti aggiornamento dell'attributo)

Le funzionalità offerte da tali policy di esempio sono:

- Policy(root_access) consente a qualsiasi utente con accesso di Amministratore di aggiornare qualsiasi valore. Si raccomanda di assegnare un numero di sequenza basso a questo tipo di policy.
- Policy(cohesion_non_autorizzato) impedisce a qualsiasi MDR della classe MDR(Cohesion) di aggiornare l'indirizzo IP dell'elemento della configurazione filtrato. L'esempio riportato a continuazione mostra come impedire l'aggiornamento dei dati ad un MDR non autorizzato.
- Policy(utente1) consente all'utente user1 di aggiornare gli elementi della configurazione del titolare, unicamente durante l'utilizzo del client Web. Questo esempio mostra come fornire a determinati utenti il controllo completo dei dati.

Filtro dell'elemento della configurazione

La policy filtra le transazioni in base alle caratteristiche dell'elemento della configurazione aggiornato. I criteri di selezione includono il nome dell'elemento della configurazione, la classe, la priorità, il tipo di servizio e la posizione.

Importante. Il filtro dell'elemento della configurazione si basa sul valore attributo dell'elemento della configurazione prima dell'aggiornamento, non sul valore dei dati della transazione in entrata.

Esempio: Policy di filtro dell'elemento della configurazione

Le seguenti policy di esempio specificano filtri dell'elemento della configurazione:

- Policy name(priorità1) filtra Service Type(risoluzione priorità1) action(Consenti aggiornamento solo in caso di corrispondenza con la specifica del Cambiamento, Crea Incidente)
- Policy name(prod-NY) filtra ci(prod*) location(NY) attribute(Tutti gli attributi gestiti) action(Consenti aggiornamento solo in caso di corrispondenza con la specifica del Cambiamento)
- Policy name(prod-not-NY) filtra ci(prod*) location(!NY) attribute(Tutti gli attributi gestiti) action(Consenti aggiornamento dell'attributo)

Le funzionalità offerte da tali policy di esempio sono:

- Policy(priority1) richiede che gli elementi della configurazione il cui tipo di servizio richiede una *risoluzione con priorità 1* dispongano di un Ordine di Cambiamento associato. Tale policy è considerata come procedura ottimale, in quanto consente di controllare i principali elementi della configurazione in CMDB. Inoltre, verifica che tutti i Cambiamenti inclusi nella gestione dei Cambiamenti dispongano di specifiche del Cambiamento e siano stati completati.
- Policy(prod-NY) richiede che gli elementi della configurazione con posizione NY dispongano di Ordini di Cambiamento associati. L'uso della posizione per filtrare le policy consente di implementare i Cambiamenti gradualmente, sito per sito.
- Policy(prod-non-NY) illustra la modalità di utilizzo del punto esclamativo per identificare elementi della configurazione con ubicazione differente da NY.

Azioni della policy

Al completamento della selezione della policy da parte della funzionalità CACF, la sezione relativa all'azione della policy determina il risultato dell'aggiornamento attributo. Tale sezione identifica la parte più importante della policy di verifica, in quanto influisce sull'integrità di CMDB e sul flusso di lavoro, le notifiche e gli Incidenti della gestione Cambiamento.

Una policy può presentare una delle seguenti condotte di aggiornamento:

Consenti aggiornamento solo in caso di corrispondenza con la specifica del Cambiamento

Applica l'aggiornamento dell'attributo in entrata all'elemento della configurazione solo se corrisponde ad una specifica di Cambiamento. Tale aggiornamento si verifica quando l'Ordine di Cambiamento si trova in stato di verifica attivo. La selezionare di questa opzione abilita Verifica di Cambiamento.

Consenti aggiornamento dell'attributo

Applica l'aggiornamento dell'attributo in entrata all'elemento della configurazione incondizionatamente. Questa opzione disattiva efficacemente tutte le verifiche di Cambiamento. Utilizzare questo comportamento per modifiche standard, quando si ha un'origine dati attendibile e autorizzato e quando non è necessario un Ordine di Cambiamento.

Annulla sempre l'intera transazione

Annulla l'aggiornamento e qualsiasi altro aggiornamento attributo presente nella transazione, anche quando esiste una specifica di Cambiamento associata. Utilizzare questo comportamento per impedire l'aggiornamento di elementi della configurazione da parte di MDR non autorizzati. Se una policy annulla una transazione, l'intera transazione viene annullata, anche se altre policy avessero acconsentito al Cambiamento.

Questo comportamento è indicato, ad esempio, per impedire ad un MDR non autorizzato di immettere un elemento della configurazione e specificare anche un nome attributo comune del tipo *Nome*.

Mantieni il valore di attributo precedente

Annulla l'aggiornamento di un determinato attributo della transazione ma consente l'aggiornamento degli altri se la loro policy lo consente. Utilizzare questo comportamento quando un MDR non è autorizzato a livello di attributo.

Una policy di verifica può richiedere la chiusura automatica degli Incidenti una volta risolte le verifiche non riuscite. La policy può, infatti, richiedere che i dati della transazione in entrata vengano copiati nell'area di lavoro transazione. Tale tipo di policy si rivela utile quando i dati provenienti da un MDR non autorizzato richiedono una revisione prima dell'aggiornamento di CMDB.

Al fine di consentire al manager della configurazione di identificare le policy CACF responsabili della creazione del record dell'area di lavoro transazione, il campo Ordine di Cambiamento dell'area di lavoro transazione è impostato sul nome della policy che lo ha creato. La scrittura dei dati nell'area di lavoro transazione è indipendente dall'aggiornamento dell'elemento di configurazione in CMDB, per cui una policy può aggiornare l'elemento della configurazione, scrivere nell'area di lavoro transazione o effettuare entrambe le azioni.

Pianificazione policy

Per le policy di verifica è possibile specificare date di attivazione e disattivazione che consentano all'amministratore della configurazione di pianificare modifiche delle policy non gestite.

Policy multiple

Con l'introduzione di nuove policy di verifica nell'ambiente e l'aumento degli attributi da gestire, anche la complessità di organizzazione delle policy aumenta, in quanto le policy cominciano ad intersecarsi le une con le altre. Ad esempio, si dispone di una policy per gli elementi della configurazione del server e di un'altra policy per gli elementi della configurazione con ubicazione NY. Sarà necessario considerare la policy appropriata per gli elementi della configurazione del server ubicati a NY. Utilizzare il numero di sequenza della policy per dare priorità ad una policy nel caso in cui siano presenti più criteri in grado di controllare un attributo. Quando si gestiscono più attributi, la possibilità che una determinata transazione sia gestita da varie policy aumenta.

Considerare le seguenti informazioni quando si dispone di più policy attive per una determinata transazione:

- Se una policy richiede la scrittura dei dati nell'area di lavoro transazione, i dati vengono scritti nell'area di lavoro transazione.
- Se una determinata policy richiede l'annullamento della transazione, la funzionalità CACF annulla l'intera transazione.

  Importante. Le funzionalità che utilizzano il servizio Web createAsset (inclusi GRLoader e CMDBf) suddividono la transazione in tre transazioni separate: due inserimenti e un aggiornamento. È possibile consentire gli aggiornamenti di ca_owned_resource, mentre gli aggiornamenti alla tabella delle estensioni dell'elemento della configurazione vengono annullati. Gli aggiornamenti degli attributi specifici della famiglia dell'elemento della configurazione nella tabella delle estensioni potrebbero essere rilevati aggiornamenti e non come inserimenti.

Esempio: Policy multiple

I seguenti esempi specificano policy multiple:

- Nome policy(Indirizzo IP) attributo(Indirizzo IP) azione(Consenti aggiornamento dell'attributo)
- Nome policy(Memoria installata) attributo(Memoria installata) azione(cancella transazione)
- Nome policy(Capacità disco) attributo(Capacità disco) azione(Mantieni il valore di attributo precedente)

Le funzionalità offerte da tali policy di esempio sono:

- Se una transazione esegue unicamente l'aggiornamento dell'indirizzo IP, l'aggiornamento viene effettuato.
- Se una transazione esegue unicamente l'aggiornamento della memoria installata, l'aggiornamento non viene effettuato.
- Se una transazione esegue l'aggiornamento dell'indirizzo IP e della memoria installata, la transazione viene annullata nell'interfaccia Web.
- Se una transazione esegue l'aggiornamento dell'indirizzo IP e della capacità del disco nell'interfaccia Web, l'indirizzo IP viene aggiornato, ma l'aggiornamento della capacità del disco non viene effettuato.
- Se una transazione esegue l'aggiornamento dell'indirizzo IP e della memoria installata nell'interfaccia Web, nessuno dei due attributi verrà aggiornato.

Consolidamento degli Incidenti

Quando una policy di verifica richiede la creazione di un Incidente, CACF è in grado di ridurre il numero di Incidenti aperti nel seguente modo:

- CACF crea un solo Incidente aperto per un elemento della configurazione, per i Cambiamenti non autorizzati. I Cambiamenti non autorizzati aggiuntivi aggiornano l'Incidente aperto per i Cambiamenti non autorizzati.
- CACF crea un solo Incidente aperto per ciascun errore di verifica della specifica del Cambiamento. Gli errori di verifica aggiuntivi per la specifica del Cambiamento aggiornano l'Incidente aperto.

Attributi gestiti

Gli attributi gestiti indicano gli attributi dell'elemento della configurazione disponibile per la verifica del Cambiamento di CACF. Per impostazione predefinita, questo elenco contiene gli attributi *Nome elemento della configurazione* e *Tutti gli attributi gestiti*. Aggiungere gli attributi dell'elemento della configurazione che si desidera gestire nella strategia di verifica del Cambiamento. Definire gli attributi gestiti nella strategia di verifica del Cambiamento nel nodo Controllo della configurazione, Attributi gestiti nella sezione CA CMDB della scheda Amministrazione.

CACF non include gli attributi non gestiti (attributi non elencati) nella verifica del Cambiamento. Tali attributi non gestiti vengono aggiornati normalmente.

Importante. La verifica del Cambiamento ignora gli attributi non gestiti e consente l'aggiornamento dell'elemento della configurazione da parte di tali attributi, salvo il caso in cui il comportamento Annulla sempre l'intera transazione sia stato impostato nella policy di verifica.

Nota: la distinzione maiuscole/minuscole nella definizione dell'attributo gestito viene applicata unicamente quando CACF esegue il confronto tra il valore pianificato della specifica del Cambiamento con i dati di transazione dell'elemento della configurazione in entrata. L'opzione per la distinzione tra maiuscole/minuscole non viene applicata ai modelli di selezione della policy, i quali applicano sempre la distinzione.

Per un elenco dei nomi di attributo dell'elemento della configurazione, consultare la Guida di riferimento tecnico di *CA CMDB*.

Stati del Cambiamento gestito

CACF utilizza gli stati del Cambiamento gestito per indicare quali stati dell'Ordine di Cambiamento vengono gestiti da CACF. CACF utilizza gli stati del Cambiamento gestito per controllare il momento e la modalità di applicazione della verifica del Cambiamento per gli aggiornamenti dell'elemento della configurazione nel sistema. È possibile personalizzare questi stati di Cambiamento in base alle esigenze della propria organizzazione.

La configurazione degli stati del Cambiamento gestito può essere eseguita dalla scheda Amministrazione di CA CMDB, nel nodo Controllo della configurazione, Stati del Cambiamento gestito.

Nota: CACF ignora gli Ordini di cambiamento il cui stato è incluso nell'elenco Stati del Cambiamento gestito.

Il seguente elenco descrive le opzioni degli stati del Cambiamento gestito:

Specifiche del Cambiamento modificabili

Specifica se è possibile modificare le specifiche di Cambiamento per un Ordine di Cambiamento. Generalmente, dopo che una richiesta di Cambiamento riceve l'approvazione, non è possibile modificare tale Richiesta e gli aggiornamenti riguarderanno soltanto l'esecuzione di un numero ridotto di opzioni di sostituzione in stato *Verifica in corso.*

Verifica del Cambiamento attiva

Specifica se i Cambiamenti rilevati per un elemento della configurazione quando l'Ordine di Cambiamento si trova in questo stato vengono tenuti in considerazione per la verifica del Cambiamento. Gli Ordini di Cambiamento e le specifiche di Cambiamento corrispondenti vengono confrontati con le transazioni in entrata per verificarne la corretta esecuzione.

CACF esegue il monitoraggio di tutti gli elementi della configurazione per qualsiasi Cambiamento applicato ai valori dell'attributo gestito corrispondenti. CACF verifica ciascun Cambiamento a livello dell'attributo per l'elemento della configurazione e ne esegue il confronto rispetto a un elenco di specifiche del Cambiamento con stato *Verifica del Cambiamento attiva*.

Quando una specifica del Cambiamento si trova in questo stato, qualsiasi specifica del Cambiamento senza elementi della configurazione specifici verrà espansa. Questa espansione si verifica quando vengono create nuove specifiche del Cambiamento mediante l'elenco degli elementi della configurazione associati all'Ordine di Cambiamento.

Quando la specifica del Cambiamento non presenta più questo stato, viene eseguito l'elenco delle specifiche del Cambiamento con stato *Imposta dopo l'esecuzione del Cambiamento*. L'azione aggiorna l'elemento della configurazione con i valori pianificati, in base a quanto specificato in ciascuna specifica di Cambiamento.

Stato di implementazione

Specifica se lo stato rappresenta uno stato quando i Cambiamenti vengono eseguiti o implementati per l'elemento della configurazione. Quando un Ordine di cambiamento entra in questo stato transitorio, i valori dell'attributo dell'elemento della configurazione vengono considerati volatili e possono essere aggiornati in funzione delle specifiche del Cambiamento in sospeso. CACF non può considerare tali Cambiamenti come non autorizzati ma, allo stesso tempo, non può tenerli in considerazione per la verifica finale. Generalmente, il processo di verifica del Cambiamento deve eseguire un confronto tra i dati dell'attributo in entrata dopo la corretta esecuzione dell'Ordine di Cambiamento.

Mostra pulsanti di sostituzione della specifica del Cambiamento

Specifica se l'analista del Cambiamento può controllare le specifiche del Cambiamento ed il livello di controllo consentito. In alcune implementazioni, l'analista del Cambiamento può modificare le specifiche del Cambiamento in base alle proprie esigenze. Per altre implementazioni, l'analista del Cambiamento può sovrascrivere (a pagina 734) o annullare (a pagina 735) la specifica del Cambiamento.

Promuovi Ordine di Cambiamento dopo la verifica

Specifica se un ordine di Cambiamento viene promosso automaticamente allo stato predefinito successivo dopo la verifica da parte di CACF di tutte le specifiche del Cambiamento.

Stati del Cambiamento gestito predefiniti

È possibile definire gli stati dell'Ordine di cambiamento durante i quali le specifiche del Cambiamento vengono create, sovrascritte, verificate o ignorate.

L'elenco seguente descrive le definizioni predefinite degli stati del Cambiamento gestito fornite in CA SDM come esempio:

RFC

Definisce le specifiche dell'Ordine di cambiamento che presentano questo stato, ma che vengono ignorate durante verifica del Cambiamento. Generalmente, i Cambiamenti dell'elemento della configurazione rilevati quando l'Ordine di cambiamento presenta questo stato vengono considerati come non autorizzati.

Approvazione in corso

Le specifiche del Cambiamento con questo stato possono essere modificate e presentano le stesse caratteristiche dello stato RFC, tuttavia non vengono incluse per la verifica.

In seguito all'approvazione dell'Ordine di cambiamento,e specifiche del Cambiamento vengono approvate come parte dello stesso processo di approvazione. CACF non consente l'esecuzione di modifiche aggiuntive alla specifica ed effettua l'auditing completo.

Implementazione in corso

Gli eventuali Cambiamenti dell'elemento della configurazione non vengono considerati come non autorizzati, né utilizzati per la verifica. È possibile modificare la definizione di questo stato del Cambiamento per consentire la verifica degli Ordini di cambiamento che presentano questo stato.

Verifica in corso

Questo stato non consente la modifica delle specifiche del Cambiamento, tuttavia gli analisti possono eseguirne la sovrascrittura. Con questo stato la verifica del Cambiamento è attiva. (a pagina 730)

Specifiche del Cambiamento

Un Ordine di cambiamento contiene le specifiche del Cambiamento che definiscono i Cambiamenti richiesti per un dell'elemento della configurazione specifico. CACF utilizza queste specifiche del Cambiamento quando l'Ordine di cambiamento entra in uno stato di verifica per validare e confermare che i Cambiamenti attuali dell'elemento della configurazione sono stati completati correttamente. È possibile creare le specifiche del Cambiamento da un Ordine di cambiamento, da un elemento della configurazione oppure dal nodo Controllo della configurazione, Specifiche del Cambiamento della sezione CA CMDB della scheda Amministrazione.

La specifica del Cambiamento contiene le seguenti sezioni principali:

N. Ordine di cambiamento

Specifica l'Ordine di cambiamento che richiede il Cambiamento.

Nome elemento della configurazione

Contiene il nome dell'elemento della configurazione che si desidera aggiornare.

È possibile lasciare il campo Nome elemento della configurazione vuoto per indicare che la specifica del Cambiamento si applica a tutti gli elementi della configurazione definiti per l'Ordine di cambiamento. Utilizzare questa opzione quando tutti gli elementi della configurazione di un Ordine di cambiamento utilizzano lo stesso attributo gestito e lo stesso valore pianificato. La specifica del Cambiamento viene applicata a tutti gli elementi della configurazione associati all'Ordine di cambiamento quando lo stato dell'Ordine di cambiamento passa a uno stato con verifica del Cambiamento attivata (noto anche come espansione).

Nome attributo

Specifica il nome dell'attributo gestito che si desidera aggiornare.

Selezionare Tutti gli attributi gestiti per consentire il Cambiamento di tutti gli attributi gestiti durante la verifica dell'Ordine di cambiamento. In questo caso è possibile aggiornare più attributi, pertanto non è possibile specificare il valore pianificato.

Valore pianificato

Indica il valore previsto per l'attributo dopo l'esecuzione del Cambiamento. Quando lo stato dell'Ordine di Cambiamento passa a uno stato di verifica e l'elemento della configurazione viene aggiornato mediante l'interfaccia Web, GRLoader o i servizi Web, CACF esegue un confronto tra il valore pianificato e i dati in entrata per stabilire una corrispondenza.

È possibile integrare caratteri speciali (a pagina 726) nel valore pianificato nel caso in cui non si disponga del valore esatto.

Stato

Specifica lo stato della specifica del Cambiamento (a pagina 732), ad esempio Verifica in sospeso.

Se non si è a conoscenza del valore pianificato e tale valore potrebbe subire modifiche, impostare lo stato della specifica del Cambiamento su Usa valore rilevato. Questo comportamento richiede che la funzionalità di rilevamento esegua l'aggiornamento dell'elemento della configurazione prima che CACF contrassegni la specifica del Cambiamento come convalidata. È possibile richiedere tale comportamento per i campi numerici e gli attributi SREL che non accettano l'asterisco come valore pianificato.

Per facilitare l'impostazione del valore pianificato, la scheda Cronologia attributo rilevato contiene un elenco di tutti i valori rilevati recentemente da MDR. L'elenco specifica inoltre se tali valori sono stati autorizzati o caricati in CMDB. Questa scheda mostra il formato, la distinzione maiuscole/minuscole e altre informazioni relative ai valori per determinare un modello del valore pianificato appropriato.

Ulteriori informazioni:

Caratteri speciali (a pagina 726)
Definizione del caricamento in blocco (a pagina 728)
Definizione di Cambiamenti in blocco (a pagina 728)
Controllo delle versioni e stato futuro dell'elemento della configurazione (a pagina 729)

Caratteri speciali

È possibile integrare caratteri speciali nel caso in cui l'utente non sia a conoscenza del valore esatto. Utilizzare il carattere jolly asterisco per ottenere la corrispondenza con qualsiasi numero di caratteri. Il modello *deve* corrispondere ai dati rilevati nella stessa sequenza e gli spazi sono significativi.

Ad esempio, immettere *10.*.*.* 0* come valore pianificato per ottenere la corrispondenza con tutti gli indirizzi IP il cui valore iniziale è pari a *10* e presentano due punti dopo i valori inclusi tra i punti.

Ad esempio, il valore di entrata server_type contiene Windows 2003 (WIN32) 5.2.Service Pack 2 (Build 3790) Intel x86. Per verificare questo valore, specificare il valore pianificato ** Service Pack 2 ** nella specifica del Cambiamento.

Una parola all'inizio del valore pianificato indica che il valore rilevato deve iniziare con tale valore. Allo stesso modo, un asterisco all'inizio del valore pianificato indica che il valore rilevato può iniziare con qualsiasi valore e finire con il valore specificato dopo l'asterisco.

La tabella seguente riporta alcuni esempi di utilizzo dell'asterisco:

Valore pianificato	Valore rilevato	Corrispondenza o Nessuna corrispondenza
a	b	Nessuna corrispondenza
a	a	Corrispondenza
a	aba	Corrispondenza
a	bab	Corrispondenza
a*	a	Corrispondenza
a*	ab	Corrispondenza
a*	ba	Nessuna corrispondenza
*a	a	Corrispondenza
*a	ab	Nessuna corrispondenza
*a	ba	Corrispondenza

Un modello che inizia con un punto esclamativo corrisponde alla negazione di tale valore. Il punto esclamativo può essere utilizzato unicamente come primo carattere del modello. Ad esempio, non è possibile utilizzare il modello 10.!*.*.*.

Per eseguire il confronto di valori numerici contenuti in valori di stringa, utilizzare i simboli maggiore (>) o minore (<) come primo carattere del valore pianificato. Nel caso in cui sia presente un punto esclamativo come primo carattere, tale simbolo dovrà corrispondere al secondo carattere.

Importante. CACF ignora i valori non numerici iniziali o finali nei modelli del valore pianificato e rilevato.

La tabella seguente riporta alcuni esempi di utilizzo del punto esclamativo e dei simboli maggiore e minore:

Valore pianificato	Valore rilevato	Corrispondenza o Nessuna corrispondenza
>200	aaa 201 bbb	Corrispondenza
>200GB	aaa 200 bbb	Nessuna corrispondenza
>200GB	300 GB	Corrispondenza
!<200GB	200 byte	Corrispondenza
!<200	200 bit	Corrispondenza

Se non si è a conoscenza del valore pianificato e tale valore potrebbe subire modifiche, impostare lo stato della specifica del Cambiamento su Usa valore rilevato. Questo comportamento richiede che la funzionalità di rilevamento esegua l'aggiornamento dell'elemento della configurazione prima che CACF contrassegni la specifica del Cambiamento come convalidata. È possibile richiedere tale comportamento per i campi numerici e gli attributi SREL che non accettano l'asterisco come valore pianificato.

Per facilitare l'impostazione del valore pianificato, la scheda Cronologia attributo rilevato contiene un elenco di tutti i valori rilevati recentemente da MDR. L'elenco specifica inoltre se tali valori sono stati autorizzati o caricati in CMDB. Questa scheda mostra il formato, la distinzione maiuscole/minuscole e altre informazioni relative ai valori per determinare un modello del valore pianificato appropriato.

Definizione del caricamento in blocco

La gestione di nuovi elementi della configurazione privi di un Ordine di cambiamento che definisca tali elementi della configurazione potrebbe generare errori negli ambienti CMDB. Considerare le seguenti informazioni durante la definizione di un numero elevato di elementi della configurazione:

- Definire una policy speciale di caricamento in blocco per consentire l'inserimento non autorizzato, limitato da ID utente, MDR o ruolo.
- Definire una policy speciale di caricamento in blocco per il reindirizzamento di tutti i nuovi elementi della configurazione nell'area di lavoro della transazione per la verifica e l'elaborazione successiva. Questa azione richiede anche la policy speciale di caricamento in blocco precedente.

Definizione di Cambiamenti in blocco

È possibile creare Cambiamenti identici per un numero elevato di elementi della configurazione, ad esempio durante la modifica della posizione di un insieme di elementi della configurazione, nel seguente modo:

1. Creare un Ordine di cambiamento.
2. Definire una specifica del Cambiamento unica che descriva il Cambiamento e lasciare il vuoto il nome dell'elemento della configurazione.
3. Associare tutti gli elementi della configurazione all'Ordine di cambiamento.

Se non si è a conoscenza dei dettagli di un Cambiamento prima dell'implementazione (ad esempio viene acquistato un nuovo server e si dispone unicamente del nome dell'elemento della configurazione), completare le operazioni seguenti:

1. Creare un Ordine di cambiamento.
2. Creare una specifica del Cambiamento indicante come nome dell'attributo Tutti gli attributi gestiti.
3. Lasciare il valore pianificato vuoto, in quanto non si dispone di tale informazione.
4. Eseguire il processo di gestione del Cambiamento per il ticket.
5. Quando l'Ordine di Cambiamento presenta uno stato di verifica attivo e viene eseguito il processo di rilevamento, i dati dell'elemento della configurazione in entrata vengono caricati nell'elemento della configurazione, se consentito dalla policy.
6. Una volta completati i rilevamenti per l'elemento della configurazione, la gestione del Cambiamento contrassegna la specifica del Cambiamento come verificata manualmente.

Attenersi alla procedura riportata di seguito nel caso vengano apportati più Cambiamenti diversi a un numero elevato di elementi della configurazione. Ad esempio durante lo spostamento di un insieme di server da una posizione a un'altra, è possibile assegnare un indirizzo IP univoco a ciascun server.

1. Creazione di un ordine di cambiamento
2. Creare un foglio di calcolo ed elencare in ciascuna riga il numero dell'Ordine di cambiamento, l'elemento della configurazione e i nuovi valori di attributo. Ciascuna riga corrisponde a una specifica del Cambiamento distinta.
3. Caricare il foglio di calcolo con GRLoader per creare le specifiche del Cambiamento richieste.
4. Promuovere l'Ordine di cambiamento e le specifiche del Cambiamento normalmente.

Nota: per ulteriori informazioni sull'utilizzo di GRLoader, consultare la *Guida di riferimento tecnico CA CMDB*.

Controllo delle versioni e stato futuro dell'elemento della configurazione

È possibile visualizzare le specifiche del Cambiamento nel modulo Dettagli elementi della configurazione della scheda Controllo delle versioni per accedere alle informazioni dettagliate e individuare l'Ordine di cambiamento e le specifiche del Cambiamento corrispondenti. Questa scheda mostra inoltre lo stato futuro dell'elemento della configurazione che verrà impostate un volta implementati i Cambiamenti. Inoltre, è possibile visualizzare snapshot dell'elemento della configurazione alla data pianificata dell'Ordine di cambiamento. Nel caso in cui l'Ordine di cambiamento non sia stato pianificato, la snapshot verrà mostrata come un Cambiamento non pianificato.

Il controllo delle versioni include le seguenti funzionalità:

- Individuazione rapida delle sovrapposizioni e dei conflitti delle specifiche del Cambiamento.
- Avvio diretto della specifica del Cambiamento e visualizzazione dei dettagli del Cambiamento mediante il collegamento Ordine di cambiamento nella colonna MDR disponibile nella visualizzazione dettagliata.
- Le snapshot che mostrano un *Cambiamento non pianificato* indicano un Cambiamento pianificato per un momento successivo non ancora definito.
- Visualizzazione del numero dell'Ordine di cambiamento sul lato destro dell'etichetta della snapshot per ciascuna specifica del Cambiamento.

- Visualizzazione di testo informativo al passaggio del mouse nel riquadro inferiore, incluse le seguenti informazioni sulla specifica del Cambiamento:
  - Numero dell'Ordine di cambiamento
  - Data del Cambiamento pianificato, nel caso in cui la specifica del Cambiamento includa una data pianificata
  - Data di completamento, se inclusa nell'Ordine di cambiamento

Modalità di funzionamento della verifica del Cambiamento

Se un utente richiede il salvataggio di un elemento della configurazione, CA SDM esegue la ricerca delle specifiche del Cambiamento applicabili e delle corrispondenze. Le informazioni seguenti descrivono una specifica del Cambiamento applicabile:

- L'elemento della configurazione nella specifica del cambiamento corrisponde a quello che viene salvato.
- Lo stato dell'Ordine di cambiamento corrisponde a uno stato del Cambiamento gestito definito con verifica del Cambiamento attiva.
- L'attributo nella specifica del Cambiamento è uguale all'attributo in corso di aggiornamento.
- La specifica del cambiamento è attiva.
- Se non è presente alcun attributo gestito in corso di aggiornamento o policy attive, il salvataggio viene eseguito normalmente.

Se i valori dei dati in entrata corrispondono esattamente a una specifica del Cambiamento, CACF considera la specifica del Cambiamento come convalidata. In base alla policy attiva, la verifica procede alla chiusura degli Incidenti creati dalla verifica del Cambiamento.

La verifica viene eseguita quando le informazioni provenienti dai client Web, i servizi Web o GRLoader aggiornano l'elemento della configurazione mentre l'Ordine di cambiamento e tutte le specifiche del Cambiamento sottostanti sono in corso di verifica. Una volta completate le verifiche per un Ordine di cambiamento, se lo si desidera è possibile promuovere automaticamente l'Ordine di cambiamento allo stato successivo.

Se i valori dei dati in entrata non corrispondono ai valori nella specifica del Cambiamento, il Cambiamento viene considerato come implementato in maniera errata o non riuscito e gli Incidenti vengono creati o aggiunti, a seconda della policy.

Ad esempio, CA SDM non è in grado di rilevare specifiche del Cambiamento applicabili, tuttavia sono presenti Ordini di cambiamento con stato *Verifica del Cambiamento attiva*. Tali Ordini di cambiamento specificano l'elemento della configurazione di destinazione e non dispongono di specifiche del Cambiamento. Per la gestione del Cambiamento, CACF utilizza le policy per la gestione di *Ordini di Cambiamento senza specifiche*.

- Se non sono presenti specifiche del Cambiamento applicabili o Ordini di cambiamento senza specifiche, l'operazione di salvataggio viene considerata come non autorizzata.
- In seguito all'elaborazione di tutti gli attributi, vengono attivate tutte le policy che richiedono la scrittura dei dati in entrata nell'area di lavoro della transazione.

Ulteriori informazioni:

Gestione delle specifiche del Cambiamento (a pagina 731)
Stati della specifica del Cambiamento (a pagina 732)
Gestione delle verifiche non riuscite (a pagina 734)
Gestione degli attributi non rilevabili (a pagina 735)

Gestione delle specifiche del Cambiamento

In seguito all'esecuzione o implementazione di un Cambiamento, l'Ordine di cambiamento entra in uno stato di Cambiamento gestito da CACF con *verifica del Cambiamento attiva*. Quando l'Ordine di cambiamento presenta questo stato, CACF verifica l'attività dell'elemento della configurazione correlato e riporta lo stato di ciascuna specifica del Cambiamento nel contatore.

Il contatore viene utilizzato dalla gestione del Cambiamento per verificare la corretta esecuzione di tutti i Cambiamenti richiesti ed eseguire le verifiche manuali richieste dagli Ordini di cambiamento.

Una volta completate tutte le verifiche per un Ordine di cambiamento, è possibile promuovere automaticamente l'Ordine di cambiamento allo stato successivo (generalmente, Chiuso) in cui tutte le specifiche del Cambiamento vengono contrassegnate automaticamente come inattive.

Stati della specifica del Cambiamento

Le specifiche del Cambiamento utilizzano lo stato per indicare il tipo di verifica da eseguire e lo stato di verifica corrente. Inoltre, i valori di stato vengono utilizzati nel registro di verifica durante la registrazione delle operazioni di verifica del Cambiamento durante il processo di verifica.

Stati di verifica iniziale

Gli stati di verifica iniziale vengono utilizzati durante la creazione di una specifica del Cambiamento per specificare il tipo di verifica che deve essere eseguita da CACF. Non si tratta di stati finali e l'Ordine di cambiamento non viene considerato come verificato nel caso in cui lo stato delle le specifiche del Cambiamento corrisponda a uno di questi stati.

Verifica in sospeso: la specifica del Cambiamento non è stata verificata, oppure il Cambiamento è in attesa dell'aggiornamento dell'elemento della configurazione.

Richiedi verifica manuale: quando i Cambiamenti per un Ordine di cambiamento sono stati verificati, viene richiesta la verifica manuale.

Usa valore rilevato: questo stato consente di copiare il valore rilevato nell'elemento della configurazione durante la verifica. Viene utilizzato nel caso in cui l'utente non sia a conoscenza del valore pianificato prima della verifica.

Imposta dopo l'esecuzione del Cambiamento: consente di impostare un attributo dell'elemento della configurazione sul valore pianificato in seguito al completamento della verifica. Utilizzare questo stato per impostare gli attributi dell'elemento della configurazione nel caso in cui l'attributo non sia rilevabile. Ad esempio, impostare il contatto primario dell'elemento della configurazione su User1 dopo il completamento di un Cambiamento.

Stati finali

Indica una specifica del Cambiamento completata e contrassegnata come finale. Quando tutte le specifiche del Cambiamento presentano uno stato finale, gli Ordini di cambiamento sono disponibili per la promozione allo stato predefinito successivo.

Verificato: la specifica del Cambiamento è stata verificata correttamente.

Verificato manualmente: la specifica del Cambiamento è stata verificata manualmente.

Valore rilevato utilizzato: l'elemento della configurazione è stato aggiornato con il valore rilevato.

Impostato come valore pianificato: l'elemento della configurazione è stato aggiornato con il valore pianificato dopo la verifica dell'Ordine di cambiamento.

Valore pianificato accettato: l'elemento della configurazione è stato aggiornato con il valore pianificato e sovrascritto durante la verifica.

Valore rilevato accettato: l'elemento della configurazione è stato aggiornato con il valore rilevato e sovrascritto durante la verifica.

Nessuna modifica: durante la verifica, il valore pianificato corrisponde all'elemento della configurazione e non è richiesta alcuna verifica.

Annulla: la specifica del Cambiamento è stata annullata (a pagina 734) dalla gestione del Cambiamento.

Stati di intervento

Indica che una specifica del Cambiamento richiede l'intervento manuale per la verifica. CA SDM evidenzia questi stati in rosso nei moduli di elenco. Non si tratta di stati finali e l'Ordine di cambiamento non viene considerato come verificato nel caso in cui lo stato delle le specifiche del Cambiamento corrisponda a uno di questi stati.

Verifica non riuscita: il valore rilevato non corrisponde al valore specificato nell'Ordine di cambiamento. L'analista del Cambiamento deve determinare se il Cambiamento è stato eseguito correttamente e l'Ordine di cambiamento non è stato specificato correttamente, oppure se l'Ordine di cambiamento è corretto il Cambiamento richiede un'ulteriore verifica. In base alla definizione dello stato del Cambiamento gestito e allo stato corrente dell'Ordine di cambiamento, l'analista del Cambiamento può sovrascrivere, modificare o annullare la specifica del Cambiamento non riuscita.

Verifica manuale attiva: la verifica manuale viene richiesta prima di contrassegnare la specifica del Cambiamento come finale.

Stati di sovrascrittura dell'azione

Indica un'azione da eseguire durante la verifica del Cambiamento. Non si tratta di stati finali e l'Ordine di cambiamento non viene considerato come verificato nel caso in cui lo stato delle le specifiche del Cambiamento corrisponda a uno di questi stati.

Accetta valore pianificato: richiede la sovrascrittura dell'attributo dell'elemento della configurazione con il valore pianificato.

Accetta valore rilevato: richiede la sovrascrittura dell'attributo dell'elemento della configurazione con il valore rilevato.

Stato di reporting

Indica il risultato delle operazioni di policy visualizzate nel registro di verifica a scopo di registrazione e non per l'utilizzo da parte delle specifiche del Cambiamento.

Aggiornamento consentito: la policy autorizza l'aggiornamento di un elemento della configurazione privo di corrispondenza con le specifiche del Cambiamento.

Gestione delle verifiche non riuscite

In caso di errore della verifica, il nodo Verifica non riuscita (CMDB, Audit di Controllo) contrassegna in rosso il numero di verifiche non riuscite e le specifiche del Cambiamento che richiedono un intervento manuale nel contatore. Inoltre è possibile visualizzare le specifiche del Cambiamento con stato Verifica non riuscita nella scheda corrispondente delle schede Ordine di cambiamento, Elemento della configurazione o Amministrazione. In caso di errore della verifica, l'analista del Cambiamento può intervenire o attendere il rilevamento successivo.

Se lo stato del Cambiamento gestito consente l'azione Mostra pulsanti di sostituzione della specifica del Cambiamento, l'analista del Cambiamento può aprire la specifica del Cambiamento, rivedere i dati e fare clic su una delle opzioni seguenti per chiudere la verifica con uno stato finale:

Accetta valore rilevato

L'analista determina che la specifica del Cambiamento non è corretta e che lo strumento di rilevamento ha individuato il valore corretto.

Accetta valore pianificato

L'analista determina che il valore individuato dallo strumento di rilevamento non è corretto oppure che lo strumento non ha eseguito il rilevamento, e decide di accettare il valore pianificato, come se fosse stato rilevato correttamente.

Annulla

Questa parte dell'Ordine di cambiamento non viene eseguita e la specifica viene annullata.

Gestione degli attributi non rilevabili

Se una specifica del Cambiamento richiede la verifica manuale, l'analista della configurazione dovrà eseguire la verifica manuale del Cambiamento. In caso di errore della verifica, il nodo Intervento manuale (CMDB, Audit di configurazione) contrassegna in rosso il numero di specifiche del Cambiamento che richiedono un intervento manuale nel contatore. Inoltre è possibile visualizzare le specifiche del Cambiamento con stato Verifica manuale attiva nella scheda corrispondente delle schede Ordine di cambiamento, Elemento della configurazione o Amministrazione.

Se lo stato del Cambiamento gestito consente l'azione Mostra pulsanti di sostituzione della specifica del Cambiamento, l'analista del Cambiamento può aprire la specifica del Cambiamento, rivedere i dati e fare clic su una delle opzioni seguenti per chiudere la verifica con uno stato finale:

Contrassegna come verificato

Utilizzare questa opzione nel caso in cui non sia possibile rilevare l'attributo e verificato manualmente.

Annulla

Questa parte dell'Ordine di cambiamento non viene eseguita e la specifica viene annullata.

Archiviazione ed eliminazione dei dati di audit

Durante le operazioni di manutenzione del database si consiglia di eseguire l'archiviazione e l'eliminazione delle voci obsolete del registro di verifica, della cronologia di audit di CACF e della cronologia di audit dell'elemento della configurazione.

Importante. Generalmente, i report CA Business Intelligence CACF includono rapporti mensili presenti con un riepilogo annuale. Il valore predefinito dell'intervallo di eliminazione per le regole di eliminazione e archiviazione per il registro, la cronologia di audit di CACF e le tabelle di cronologia di audit dell'elemento della configurazione è di 30 giorni. L'utilizzo dello stesso valore per le regole di eliminazione e archiviazione garantisce la coerenza dei dati delle voci del registro di verifica, degli Incidenti e degli Ordini di cambiamento. È possibile modificare il valore predefinito di 30 giorni in base ai requisiti di reporting.

Completare le azioni seguenti per eseguire l'archiviazione e l'eliminazione dei dati di audit:

1. Utilizzare la regola di Incidente corrente per l'archiviazione e l'eliminazione degli Incidenti non attivi da più di *nn* giorni.

   CA SDM archivia ed elimina le voci del registro di verifica solo dopo aver archiviato ed eliminato gli Incidenti associati. Se un Ordine di cambiamento viene associato a un Incidente, CA SDM non verifica se l'Ordine di cambiamento è attivo.

2. Utilizzare la regola di Ordine di cambiamento corrente per archiviare ed eliminare gli Ordini di cambiamento non attivi da più di *nn* giorni.

   CA SDM archivia ed elimina le voci del registro di verifica e le specifiche del Cambiamento solo dopo aver archiviato ed eliminato gli Ordini di cambiamento associati. Se un Incidente viene associato a un Ordine di cambiamento, CA SDM non esegue l'archiviazione e l'eliminazione dell'Ordine di cambiamento.

3. Utilizzare la regola Registro della verifica del Cambiamento non autorizzato per i Cambiamenti non autorizzati che non hanno creato Incidenti.

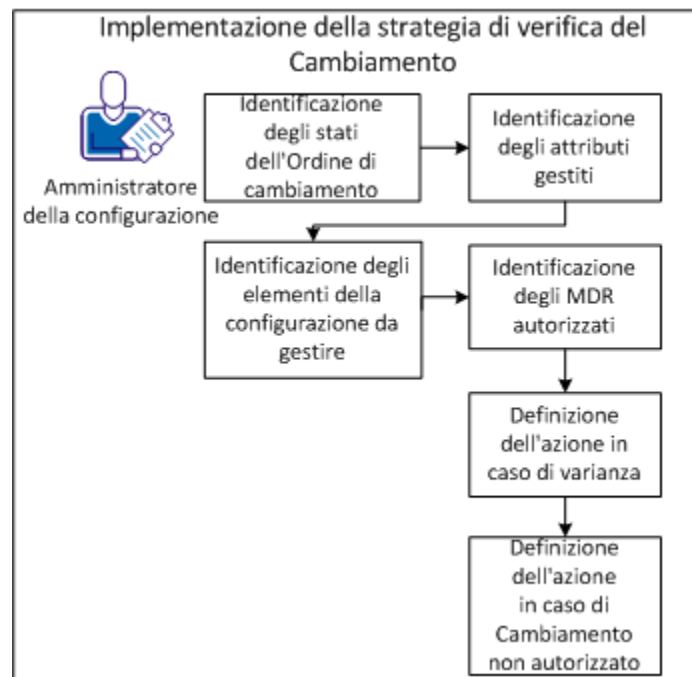
   Utilizzare questa regola per archiviare ed eliminare le voci del registro di verifica registrate da più di *nn* giorni. Per definizione, i Cambiamenti non autorizzati non vengono associati agli Ordini di cambiamento.

4. Utilizzare la regola Audit CMDB per archiviare le informazioni mostrate nelle schede Cronologia Specifiche del Cambiamento, Cronologia Policy di verifica, Cronologia Stato del Cambiamento gestito e Cronologia attributo gestito incluse nei relativi moduli dei dettagli Specifiche del Cambiamento, Policy di verifica, Stati del Cambiamento gestito e Attributi gestiti. CA SDM archivia le informazioni nella tabella ci_audit.

Implementazione della strategia di verifica del Cambiamento.

L'amministratore della configurazione determina il livello di implementazione della strategia di verifica del Cambiamento per il l'ambiente CMDB in uso. Individuare le aree del processi di gestione del Cambiamento che richiedono una strategia di verifica del Cambiamento. Tali aree includono gli attributi controllati dal Cambiamento, gli stati dell'Ordine di cambiamento che indicano se la verifica del Cambiamento è attiva, le condizioni per la modifica della specifica del Cambiamento e gli MDR autorizzati.

Ad esempio, si desidera consentire unicamente gli aggiornamenti dell'attributo dell'indirizzo IP da MDR1. Definire le azioni da eseguire quando CACF individua una varianza e un Cambiamento non autorizzato.

Il diagramma seguente descrive il processo di implementazione di una strategia di verifica del Cambiamento da parte di un amministratore della configurazione:

1. Identificazione degli stati dell'Ordine di cambiamento (a pagina 738).
2. Identificazione degli attributi gestiti (a pagina 738).
3. Identificazione degli elementi della configurazione da gestire (a pagina 739).
4. Identificazione degli MDR autorizzati (a pagina 740).
5. Definizione dell'azione in caso di varianza (a pagina 741).
6. Definizione dell'azione in caso di Cambiamento non autorizzato (a pagina 741).

Identificazione degli stati dell'Ordine di cambiamento

L'amministratore della configurazione identifica gli stati dell'Ordine di cambiamento nel caso in cui la verifica di Cambiamento sia attiva per l'elemento della configurazione in seguito all'esecuzione di un Cambiamento. Gli stati del Cambiamento consentono di definire condizioni specifiche, ad esempio la possibilità di apportare modifiche alle specifiche del Cambiamento con uno stato determinato. Ad esempio, si desidera rivedere lo stato del Cambiamento RFC per gli Ordini di cambiamento che richiedono l'aggiornamento degli elementi della configurazione.

Procedere come descritto di seguito:

1. Nella scheda Amministrazione, fare clic su CA CMDB, Controllo della configurazione e Stati del Cambiamento gestiti.
2. Fare clic su RFC per visualizzare i dettagli dello stato del Cambiamento o creare uno stato dell'Ordine di cambiamento non ancora definito.

   Nota: per impostazione predefinita, lo stato dell'Ordine di cambiamento RFC consente solo la modifica delle specifiche del Cambiamento. Lo stato Implementazione in corso non consente la modifica delle specifiche del Cambiamento. Lo stato Verifica in corso abilita la verifica del Cambiamento e mostra i pulsanti di sovrascrittura per il manager del Cambiamento o l'utente autorizzato.
3. Specificare le opzioni e il comportamento della funzionalità CACF per gli Ordini di cambiamento con questo stato.
4. Fare clic su Salva.

Identificazione degli attributi gestiti

Identificare gli attributi dell'elemento della configurazione che si desidera gestire per la strategia di verifica del Cambiamento. Ad esempio, si desidera gestire l'attributo Indirizzo IP (alarm_id) attributo con la verifica del Cambiamento.

Procedere come descritto di seguito:

1. Nella scheda Amministrazione, fare clic su CA CMDB, Controllo della configurazione e Attributi gestiti.
2. Fare clic su Crea nuovo.
3. Completare le fasi seguenti:
   a. Immettere **alarm_id** come nome dell'attributo.
   b. Immettere **indirizzo IP** come etichetta dell'attributo.

c. Selezionare uno stato di verifica iniziale dall'elenco a discesa.

   Impostazione predefinita: Verifica in sospeso

d. (Facoltativo) Selezionare l'opzione Distinzione maiuscole/minuscole se si desidera applicare la distinzione tra maiuscole e minuscole nel confronto tra i valori pianificati della specifica del Cambiamento.

   Impostazione predefinita: Disattivato

e. Fare clic su Salva.

Identificazione degli elementi della configurazione da gestire

Identificare gli elementi della configurazione che si desidera gestire mediante una policy di verifica. Ad esempio, si desidera gestire l'indirizzo IP (alarm_id) per tutti gli elementi della configurazione con priorità alta e il cui nome inizia per NY_Server.

Procedere come descritto di seguito:

1. Nella scheda Amministrazione, fare clic su CA CMDB, Controllo della configurazione e Policy di verifica.
2. Fare clic su Crea nuovo.
3. Completare le fasi seguenti:
   a. Immettere una sequenza, ad esempio **100**.
   b. Immettere**NY Server IP Addresses** come nome della policy.
   c. Selezionare le opzioni di allineamento dell'Ordine di cambiamento appropriate.

      Ad esempio, si desidera applicare la policy di verifica a tutte le opzioni salvo gli Ordini di cambiamento privi di specifiche.
4. Completare le seguenti operazioni per specificare i filtri dell'elemento della configurazione e la transazione:
   a. Selezionare Indirizzo IP dall'elenco a discesa Attributo gestito.
   b. Immettere un modello di ruolo oppure utilizzare l'asterisco per tutti i ruoli.

c. Immettere **NY** come modello di posizione.

d. Immettere **NY_Server*** come nome di modello dell'elemento della configurazione.

   Ad esempio, questo filtro verifica gli elementi della configurazione denominati NY_Server1, NY_Server2, eccetera.

5. Selezionare *Consenti aggiornamento solo in caso di corrispondenza con la specifica del Cambiamento* dall'elenco a discesa Comportamento di aggiornamento.
6. (Facoltativo) Utilizzare l'opzione Modalità Solo accesso se desidera eseguire esperimenti con la policy e visualizzare i risultati soltanto nel registro standard, senza compromettere l'ambiente CMDB attivo.
7. Fare clic su Salva.

Identificazione degli MDR autorizzati

Identificare gli MDR autorizzati nell'ambiente CMDB in uso. Ad esempio, si desidera consentire gli aggiornamenti degli elementi della configurazione da CA Configuration Automation identificati come MDR1. Si considerano gli aggiornamenti dai servizi Web identificati come MDR2 come non autorizzati e si desidera inviare le richieste all'Area di lavoro della transazione.

Procedere come descritto di seguito:

1. Aprire la policy Indirizzo IP del server NY, quindi fare clic su Modifica.
2. Immettere **MDR1** come modello del nome MDR.

   Nota: Se si desidera escludere un MDR denominato MDR2 ma si desidera consentire MDR, MDR3 e così via, specificare **!MDR2** come modello.

3. Creare una policy di verifica separata, come ad esempio Server MDR2 NY.
4. Immettere le stesse informazioni specificate per la policy precedente, fatta eccezione per i seguenti campi:

   a. Immettere **MDR2** come modello del nome MDR.

   b. Selezionare *Annulla sempre l'intera transazione* come comportamento di aggiornamento.

   c. Selezionare Sempre dall'elenco a discesa Esegui la scrittura dei dati nell'area di lavoro della transazione.

5. Fare clic su Salva.

Definizione dell'azione per una varianza

Definire l'azione per una varianza. Ad esempio, un Cambiamento dell'elemento della configurazione non corrisponde ai valori specificati nell'Ordine di Cambiamento. Si desidera che la policy di verifica crei un Incidente per la varianza.

Procedere come descritto di seguito:

1. Aprire la policy Server MDR2 NY creata e fare clic su Modifica.
2. Selezionare Sì dall'elenco a discesa Crea Incidente ed assegnare un modello.
3. Fare clic su Salva.
4. Un utente finale crea un Ordine di cambiamento con una specifica del Cambiamento per aggiornare un elemento della configurazione da MDR2.
5. CACF crea un Incidente se MDR2 richiede un aggiornamento degli elementi della configurazione con un valore non corrispondente al valore pianificato nella specifica del Cambiamento definita nell'Ordine di cambiamento.

Definizione dell'azione per un Cambiamento non autorizzato.

Definire l'azione per un Cambiamento non autorizzato. Ad esempio, CACF rileva un Cambiamento apportato a un elemento della configurazione che non dispone di specifiche di Cambiamento negli Ordini di cambiamento attivi. L'amministratore della configurazione desidera rifiutare questi tipi di richiesta.

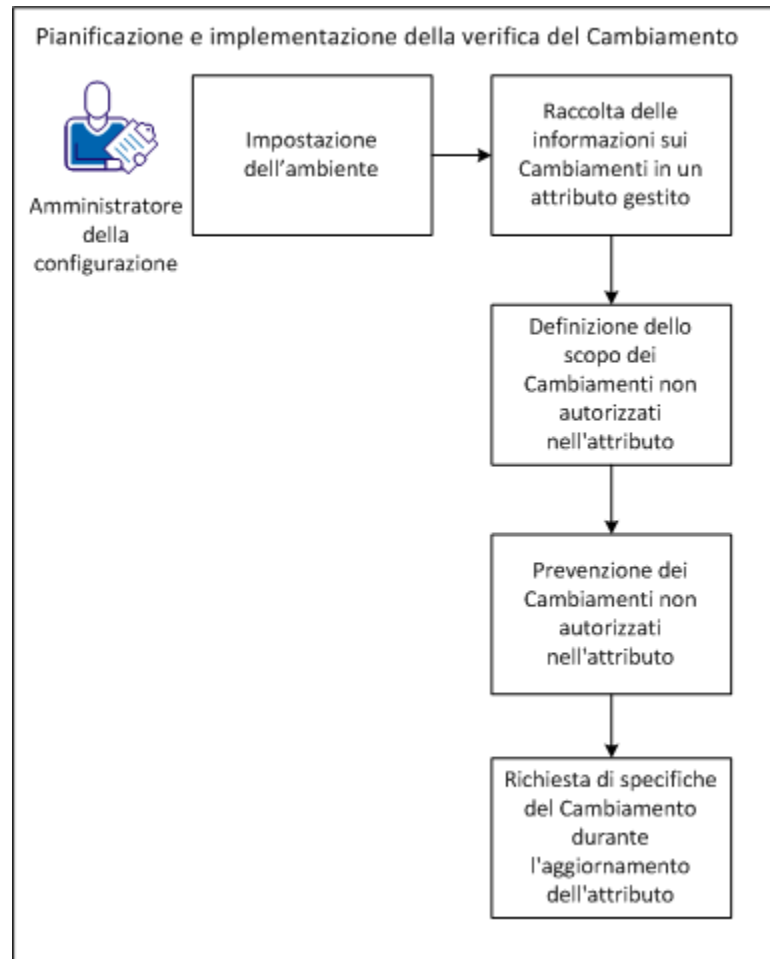
Procedere come descritto di seguito:

1. Creare una policy di verifica e specificare **Server NY non autorizzato** come nome.
2. Completare i campi di modello appropriati.
3. Verificare che siano selezionate soltanto le opzioni Inserimento non autorizzato e Aggiornamento non autorizzato per l'allineamento dell'ordine di Cambiamento.
4. Selezionare *Consenti aggiornamento solo in caso di corrispondenza con la specifica del Cambiamento* dall'elenco a discesa Comportamento di aggiornamento.
5. Selezionare Sì dall'elenco a discesa Crea Incidente ed assegnare un modello.
6. Fare clic su Salva.

Progettazione e implementazione della verifica di Cambiamento.

Il manager della configurazione desidera implementare la verifica di Cambiamento in modo che CMDB contenga i dati corretti. Il manager del Cambiamento desidera verificare che i Cambiamenti vengano eseguiti correttamente. Desidera inoltre identificare i Cambiamenti non autorizzati, quantificarne il numero e stabilire le fonti di dati corrispondenti. Entrambi i manager concordano che l'implementazione della verifica di Cambiamento apporti valore significativo all'organizzazione. Il Manager del Cambiamento desidera garantire che ogni Cambiamento apportato al processo di Gestione Cambiamento non danneggi l'ambiente di produzione.

Il manager della configurazione e il manager dei Cambiamenti approvano un'implementazione per fasi in modo tale che l'amministratore della configurazione possa implementare le policy per posizioni ed elementi della configurazione specifici per tali posizioni. Il presente scenario descrive le fasi di esempio relative al completamento dell'implementazione della policy di verifica volta a un pubblico più ampio per la propria organizzazione.

Il diagramma seguente mostra la procedura di completamento eseguita da un amministratore della configurazione relativa alle fasi di esempio per l'implementazione della verifica del Cambiamento:

1. Impostazione dell'ambiente (a pagina 744).
2. Raccolta di informazioni relative ai Cambiamenti apportati all'attributo gestito (a pagina 744).
3. Definizione dell'ambito dei Cambiamenti non autorizzati apportati all'attributo (a pagina 746).
4. Blocco dei Cambiamenti non autorizzati per l'attributo (a pagina 747).
5. Richiesta di specifiche di Cambiamento durante l'aggiornamento dell'attributo (a pagina 748).

Impostazione dell'ambiente

Viene impostato l'ambiente in modo che gli amministratori della configurazione possano sempre aggiornare gli elementi della configurazione. L'amministratore della configurazione può creare e aggiornare gli elementi della configurazione in CMDB in base alle proprie necessità senza dover specificare un Ordine di cambiamento. I dati dell'elemento della configurazione forniti vengono considerati attendibili.

Procedere come descritto di seguito:

1. Creare una policy di verifica denominata **Policy0.1** con le seguenti informazioni:
   - Specificare **1** come sequenza.
   - Specificare **Consenti sempre agli amministratori di aggiornare gli elementi della configurazione** come descrizione.
   - Selezionare tutte le opzioni di allineamento dell'ordine di Cambiamento.
   - Specificare **Amministratore della configurazione** come modello del ruolo.
   - Specificare **client Web** come modello della classe MDR.
   - Immettere un asterisco (*****) per il nome e la classe dell'elemento della configurazione, nonché per tutti gli altri modelli.
   - Selezionare Tutti gli attributi gestiti per l'attributo gestito.
2. Selezionare Consenti aggiornamento dell'attributo come azione del comportamento di aggiornamento.
3. Fare clic su Salva.

   La policy viene abilitata per consentire l'aggiornamento degli elementi della configurazione soltanto agli amministratori della configurazione.

Raccolta di informazioni relative ai Cambiamenti apportati all'attributo gestito

Si desidera raccogliere informazioni relative ai Cambiamenti apportati a un attributo dell'elemento della configurazione specifico, gli elementi della configurazione aggiornati, le fonti dei Cambiamenti, l'autore dei Cambiamenti e i valori specificati per la definizione di una strategia di verifica per gli attributi e gli elementi della configurazione corrispondenti. Ad esempio, si desidera stabilire l'ambito di tutti i Cambiamenti apportati all'indirizzo IP (alarm_id) e registrare i dati nel registro standard di CA SDM (sdtlog). La raccolta di queste informazioni potrebbe richiedere alcune settimane in base al numero di Cambiamenti apportati agli attributi all'interno della propria organizzazione.

1. Definire l'indirizzo IP (alarm_id) come attributo gestito.
2. Definire Implementazione in corso e Verifica in corso come stati del Cambiamento gestito dell'ambiente in uso, quindi abilitare l'opzione Verifica del cambiamento attiva.

3. Creare una policy di verifica denominata **Policy1.1** con le seguenti informazioni:
   - Specificare **3000** come sequenza.
   - Immettere **Registrazione di tutti i Cambiamenti apportati all'indirizzo IP** come descrizione.
   - Selezionare tutte le opzioni di allineamento dell'ordine di Cambiamento.
   - Immettere un asterisco (*) per il nome e la classe dell'elemento della configurazione, nonché per tutti gli altri modelli.
   - Abilitare la modalità di sola registrazione.
4. Fare clic su Salva.
5. Una volta trascorse alcune settimane, revisionare i registri stdlogs per visualizzare le fonti degli aggiornamenti.

   Ad esempio, il registro contiene gli aggiornamenti non autorizzati e gli aggiornamenti con Ordini di Cambiamento corrispondenti.
6. I dati consentono di stabilire che gli utenti situati a New York hanno aggiornato l'indirizzo IP degli elementi della configurazione senza aver creato gli Ordini di cambiamento.
7. Dopo avere completato l'analisi, disattivare la policy Policy 1.1 modificando la policy e sostituendo l'impostazione Attivo? con Non attivo.

Definizione dell'ambito dei Cambiamenti non autorizzati apportati all'attributo

Si desidera determinare l'ambito dei Cambiamenti non autorizzati per l'attributo Indirizzo IP. La definizione dell'ambito dei Cambiamenti non autorizzati consente di stabilire l'impatto di tali Cambiamenti sull'organizzazione. Ad esempio, riprendendo l'analisi precedente ottenuta mediante l'opzione Modalità Solo accesso, è possibile creare Incidenti ogni volta che l'indirizzo IP viene modificato con un elemento della configurazione che inizia per "test" situato a New York senza Ordine di cambiamento. Contattare i manager del Cambiamento della propria organizzazione per ignorare i nuovi Incidenti creati dal processo.

Procedere come descritto di seguito:

1. Completare le seguenti azioni di implementazione iniziali:
   - Definire Implementazione in corso come stato del Cambiamento gestito e abilitare l'opzione Stato implementazione.
   - Definire Verifica in corso come lo stato di Cambiamento gestito e disattivare l'opzione Promuovi Ordine di Cambiamento dopo la verifica. .
   - Definire l'indirizzo IP (alarm_id) come attributo gestito (qualora non sia già stato definito).
2. Creare una policy di verifica denominata Policy2.1 con le seguenti informazioni:
   - Specificare 3001 come sequenza.
   - Immettere una descrizione per la policy. Ad esempio, viene immesso **Creazione di Incidenti in caso di inserimenti e aggiornamenti non autorizzati. Tutti gli altri Cambiamenti non verranno autorizzati**.
   - Selezionare Inserimenti non autorizzati e Aggiornamenti non autorizzati come allineamenti.
   - Selezionare Indirizzo IP dall'elenco a discesa Attributo gestito.
   - Immettere **test*** come nome dell'elemento della configurazione, **NY** come posizione e un asterisco per tutti gli altri modelli.
   - Selezionare Consenti aggiornamento dell'attributo, Sì per l'azione Crea Incidente e un modello di Incidente.
3. Fare clic su Salva.

   Una volta completata questa fase, CACF crea gli Incidenti per tutti i computer di NY. Dopo aver revisionato gli Incidenti, vengono visualizzate le seguenti informazioni:

   - Molti MDR riportano diversi indirizzi IP per lo stesso elemento della configurazione.
   - Alcuni MDR sono autorizzati mentre altri non lo sono.
   - Potrebbe non essere possibile gestire alcuni elementi della configurazione in base al tipo di posizione, di famiglia, di nome, di servizio e così via.

4. Il manager del Cambiamento si riunisce con altri manager IT per verificare CMDB, i moduli di dettaglio dell'elemento della configurazione, i registri di verifica e filtrare i dati in base al nome dell'attributo per visualizzare i dati non autorizzati.
5. All'interno della propria organizzazione si decide di aggiornare il filtro dell'elemento della configurazione in Policy 2.1 in modo da gestire soltanto i server con priorità 1.

Blocco dei Cambiamenti non autorizzati per l'attributo

Si desidera impedire l'applicazione di Cambiamenti non autorizzati sull'indirizzo IP dell'attributo, in modo da garantire l'integrità dei dati di CMDB e richiedere un Ordine di cambiamento per l'aggiornamento. L'Ordine di cambiamento dovrà specificare l'elemento della configurazione e non verrà richiesta una specifica di Cambiamento per l'indirizzo IP in modo che il Cambiamento possa verificarsi. La verifica del Cambiamento si produce a livello dell'elemento della configurazione o dell'Ordine di Cambiamento, ma non a livello dell'attributo. Ad esempio, impedire tutti gli aggiornamenti non autorizzati e utilizzare la creazione degli Incidenti per monitorare gli utenti che richiedono tali Cambiamenti.

Procedere come descritto di seguito:

1. Impostare Policy 1.1 e Policy 2.1 su Non attivo per disattivarle.
2. Creare Policy 3.1 con le seguenti informazioni:
   - Specificare **3100** come sequenza.
   - Immettere **Blocco dei Cambiamenti non autorizzati senza Ordine di cambiamento** come descrizione.
   - Selezionare Aggiornamento non autorizzato come allineamento.
   - Immettere **test*** come nome dell'elemento della configurazione, **NY** come posizione, Tutti gli attributi gestiti come attributo e un asterisco per tutti gli altri modelli.
   - Selezionare l'azione Annulla sempre l'intera transazione.
3. Fare clic su Salva.
4. Creare Policy 3.2 con le seguenti informazioni:
   - Specificare **3200** come sequenza.
   - Immettere **Ordine di cambiamento obbligatorio per i Cambiamenti all'indirizzo IP** come descrizione.
   - Selezionare Ordini di cambiamento senza specifiche come allineamento.
   - Immettere **test*** come nome dell'elemento della configurazione, **NY** come posizione e un asterisco per tutti gli altri modelli.

- Selezionare Indirizzo IP dall'elenco a discesa Attributo gestito.
- Selezionare Consenti aggiornamento dell'attributo come azione.

5. Fare clic su Salva.

   La policy elimina i Cambiamenti non autorizzati poiché gli Ordini di Cambiamento devono essere associati al Cambiamento.

   Il manager della configurazione constata che i dati non definiti nell'Ordine di cambiamento sono stati comunque aggiornati, in quanto le specifiche di Cambiamento non sono obbligatorie a livello di attributo. Ad esempio, la richiesta di un Cambiamento per l'aumento della memoria installata contemporaneamente al Cambiamento dell'indirizzo IP non verrà considerato un Cambiamento non autorizzato in quanto è presente un Ordine di cambiamento. I manager desiderano inoltre che gli Ordini di cambiamento vengano verificati e promossi automaticamente, e stabiliscono che la verifica verrà eseguito a livello dell'attributo.

Richiesta di specifiche di Cambiamento durante l'aggiornamento dell'attributo

Il manager della configurazione constata che i dati di CMDB ricevono aggiornamenti multipli per i Cambiamenti non specificati nell'Ordine di cambiamento. Ad esempio, un utente modifica il valore della memoria installata (phys_mem) e l'indirizzo IP (ip_address) contemporaneamente. Nella fase precedente, CACF non considera questa richiesta come Cambiamento non autorizzato in quanto esiste un Ordine di Cambiamento.

Il manager della configurazione desidera potenziare la verifica del Cambiamento a livello di attributo. L'amministratore della configurazione crea una policy che richiede l'utilizzo di specifiche di Cambiamento durante l'aggiornamento dell'indirizzo IP e la creazione di un Incidente nel caso in cui non siano stati eseguiti aggiornamenti non autorizzati.

Procedere come descritto di seguito:

1. Il manager della configurazione contatta gli analisti del Cambiamento e comunica loro che i Cambiamenti apportati all'indirizzo IP dovranno contenere una specifica del Cambiamento.
2. Impostare Policy 3.1 e Policy 3.2 su Non attivo per disattivare le policy.
3. Creare la policy Policy 4.1 con le seguenti informazioni:
   - Specificare **4000** come sequenza.
   - Immettere **Specifiche di Cambiamento obbligatorie per i Cambiamenti all'indirizzo IP** come descrizione.
   - Selezionare Inserimento non autorizzato, Aggiornamento non autorizzato e Ordini di cambiamento senza specifiche come allineamento.

- Immettere **test*** come nome dell'elemento della configurazione, **NY** come posizione e un asterisco per tutti gli altri modelli.
- Selezionare Indirizzo IP dall'elenco a discesa Attributo gestito.
- Selezionare l'azione Annulla sempre l'intera transazione.

4. Fare clic su Salva.
5. Creare la policy Policy 4.2 con le seguenti informazioni:
    - Specificare **4100** come sequenza.
    - Immettere **Specifiche di Cambiamento obbligatorie per i Cambiamenti all'indirizzo IP** come descrizione.
    - Selezionare Ordini di Cambiamento con specifiche come allineamento.
    - Immettere **test*** come nome dell'elemento della configurazione e **NY** come modello della posizione.
    - Selezionare Indirizzo IP dall'elenco a discesa Attributo gestito.
    - Selezionare Consenti aggiornamento solo in caso di corrispondenza con la specifica del Cambiamento.
6. Fare clic su Salva.

Le fasi di esempio dell'implementazione della verifica del Cambiamento sono state completate correttamente. È possibile espandere la strategia di verifica del Cambiamento per includere ulteriori attributi, elementi della configurazione, MDR e titolari.

Procedure consigliate di verifica dei Cambiamenti

Durante l'implementazione della verifica del Cambiamento, tenere presente le seguenti procedure consigliate:

- Definire un numero ridotto di policy.
- Evitare l'uso della logica negativa (punto esclamativo in un modello di policy).
- Un singolo salvataggio di aggiornamento dell'elemento della configurazione deve corrispondere a un numero ridotto di policy.
- Organizzare le policy in una struttura numerica a più livelli.
- Utilizzare le policy Modalità Solo accesso prima di eseguire l'implementazione di una policy di verifica del Cambiamento.
- Ridurre il numero di policy sovrapposte, ovvero policy multiple che gestiscono un singolo attributo di aggiornamento.
- Limitare il numero di Incidenti creati da CACF.
- Implementare l'archiviazione e l'eliminazione dei dati CACF.

Ulteriori informazioni:

Organizzazione delle policy (a pagina 750)
Considerazioni su Multi-Tenancy (a pagina 751)
Accessi funzionali e ruoli CACF (a pagina 751)

Organizzazione delle policy

Per tenere traccia delle policy è possibile utilizzare diverse strategie. Si consiglia di utilizzare un approccio a livelli multipli. Utilizzare aumenti di 100 per i numeri di policy in modo da consentire gli inserimenti futuri.

Considerare i seguenti esempi a più livelli per la strategia:

Policy fondamentali

100 000 - 199 999

- Consente agli amministratori del Cambiamento di eseguire inserimenti
- Disattivare gli inserimenti per la classe MDR Class(xxxx)
- Esclude tutti gli elementi della configurazione di test dalla creazione dell'Incidente

Policy temporanee o transitorie

200 000 - 299 999: caricamenti in blocco della settimana corrente

Policy specifiche di un'applicazione

- 301 000 - 301 999: Eccezioni alle policy di applicazione generale seguenti:

  Ad esempio, le policy server1 a New York.
- 311 000 - 311 999: policy associate al tipo di servizio Risoluzione della priorità 1
- 320 000 - 320 999: policy associate a New York
- 331 000 - 331 999: policy associate a Lisle

Policy di tecnologia specifiche

- 410 000 - 410 999: policy associate ai server.
- 411 000 - 411 999: policy associate alla rete

Policy predefinite

Se le policy precendenti non vengono applicate al proprio ambiente, è possibile utilizzare le policy predefinite.

900 000 - 999 999: policy predefinite, come ad esempio tutti gli aggiornamenti agli attributi gestiti (Tutti gli attributi gestiti) devono essere associati a una specifica di Cambiamento.

Considerazioni su Multi-Tenancy

Quando CACF viene utilizzato in un ambiente multi-tenancy, è necessario tenere presenti le seguenti considerazioni:

- Gli attributi gestiti, le policy di verifica, gli Ordini di cambiamento e le specifiche di Cambiamento presentano un titolare.
- I titolari possono visualizzare tutti gli oggetti CACF all'interno della propria gerarchia.

  Ad esempio, se un titolare crea un attributo gestito, questa azione potrebbe impedire al titolare della gerarchia di creare un attributo gestito duplicato. La gerarchia richiede numeri di sequenza di policy univoci.
- Per determinare la policy di gestione di un Cambiamento apportato a un attributo, considerare soltanto le policy provenienti dalla gerarchia dei titolari dell'oggetto (elemento della configurazione).
- Un titolare secondario può creare una policy che sostituisce il titolare principale mediante l'assegnazione di un numero di sequenze ridotte rispetto alle policy locali.
- CACF considera soltanto le policy a livello di titolare e gli elementi padre corrispondenti nella gerarchia.
- CACF non tiene in considerazione il titolare del contatto autore del Cambiamento.

  Nota: le policy di verifica sono specifiche del sistema o non variano in base all'utente o al ruolo.

Accessi funzionali e ruoli CACF

La tabella seguente descrive i ruoli predefiniti utilizzati da CACF:

Ruolo/Accesso funzionale	Amministrazione	Elemento della configurazione	Incidente/Problema/Richiesta	Ordine di cambiamento
Amministratore	Modifica	Modifica	Modifica	Modifica
Amministratore della configurazione	Modifica	Modifica	Modifica	Modifica
Analista della configurazione	Visualizza	Modifica	Modifica	Modifica
Visualizzatore della configurazione	None	Visualizza	Modifica	Visualizza
Gestione Cambiamento	Visualizza	Modifica	Modifica	Modifica
Amministratore Service Desk	Modifica	Modifica	Modifica	Modifica

Ruolo/Accesso funzionale	Amministrazione	Elemento della configurazione	Incidente/Problema/Richiesta	Ordine di cambiamento
Gestione Service Desk	Visualizza	Modifica	Modifica	Modifica
Amministratore del sistema	Modifica	Modifica	Visualizza	Visualizza
Analista di livello 1	Visualizza	Visualizza	Modifica	Visualizza
Analista di livello 2	Visualizza	Modifica	Modifica	Modifica
Gestione incidente	Visualizza	Visualizza	Modifica	Modifica
Gestione problemi	Visualizza	Visualizza	Modifica	Modifica

Amministrazione

Indica i diritti di creazione, aggiornamento e visualizzazione per gli strumenti della gestione degli attributi, di policy e dell'amministrazione CACF.

Elemento della configurazione

Indica la creazione, l'aggiornamento e la visualizzazione dell'elemento della configurazione, nonché i dati di attributo della relazione.

Incidente/Problema/Richiesta

Indica i diritti di modifica e di visualizzazione dei Problemi CACF in attesa, compresi i Cambiamenti non autorizzati e le varianze di esecuzione del Cambiamento non corretto.

Ordini di cambiamento

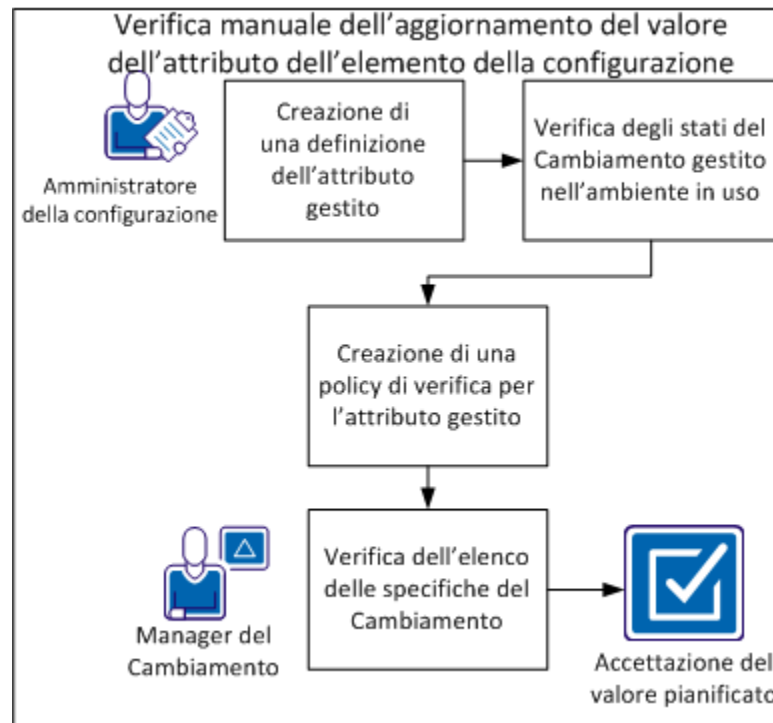
Indica la creazione, l'aggiornamento e la visualizzazione delle specifiche di Cambiamento.

Ad esempio, il ruolo di manager del Cambiamento può visualizzare le policy CACF e gestire gli attributi ma non può aggiornarli.

Importante L'accesso dell'aggiornamento all'Ordine di cambiamento e allo stato corrispondente stabilisce gli utenti che possono modificare le specifiche del Cambiamento. Ad esempio, l'amministratore del Cambiamento fornisce l'accesso al Manager del Cambiamento.

Verifica manuale di aggiornamento del valore dell'attributo dell'elemento della configurazione

L'amministratore della configurazione stabilisce che l'ambiente CA SDM richiede una policy di verifica per l'attributo Memoria installata (phys_mem). L'amministratore della configurazione crea una definizione dell'attributo gestito con stato *Richiedi verifica manuale* poiché CA SDM non dispone di un MDR per il rilevamento del valore. L'amministratore della configurazione revisione gli stati gestiti e crea una policy di verifica. Il manager del Cambiamento visualizza un ordine di Cambiamento che richiede un aggiornamento del valore Memoria installata di un elemento della configurazione e la richiesta di Cambiamento richiede la verifica manuale.

Il seguente diagramma descrive la modalità di definizione di una policy di verifica da parte dell'amministratore della configurazione e la modalità di verifica manuale eseguita dal manager del Cambiamento dell'aggiornamento di un valore di attributo dell'elemento della configurazione.

1. Creazione di una definizione dell'attributo gestito (a pagina 754).
2. Verifica degli stati del Cambiamento gestito nell'ambiente in uso (a pagina 755).
3. Creazione di una policy di verifica per l'attributo gestito (a pagina 755).
4. Verifica dell'elenco delle specifiche del Cambiamento (a pagina 757).
5. Accettazione del valore pianificato (a pagina 758).

Creazione di una definizione dell'attributo gestito

L'amministratore della configurazione crea una definizione dell'attributo gestito per l'attributo Memoria installata (phys_mem).

Procedere come descritto di seguito:

1. Nella scheda Amministrazione, fare clic su CA CMDB, Controllo della configurazione e Attributi gestiti.
2. Fare clic su Crea nuovo.
3. Immettere **phys_mem** come nome dell'attributo.
4. Immettere **Memoria installata** come etichetta dell'attributo.
5. Selezionare *Richiedi verifica manuale* dall'elenco a discesa Stato verifica iniziale.
6. (Facoltativo) Selezionare l'opzione Distinzione maiuscole/minuscole se si desidera applicare la distinzione tra maiuscole e minuscole nel confronto tra i valori pianificati della specifica del Cambiamento.

   Impostazione predefinita: Disattivato

7. Fare clic su Salva.

   L'attributo gestito viene salvato.

Verifica degli stati del Cambiamento gestito nell'ambiente in uso

L'amministratore della configurazione verifica gli stati del Cambiamento gestito nell'ambiente CA SDM. La verifica del Cambiamento viene avviata quando lo stato di un Ordine di modifica viene modificato in uno stato gestito da CACF, ad esempio Verifica in corso.

Nota: L'amministratore della configurazione può personalizzare lo stato del ciclo di vita dell'Ordine di cambiamento che avvia la verifica del Cambiamento. Inoltre, l'amministratore può personalizzare gli stati che consentono all'utente di modificare le specifiche del Cambiamento all'avvio dell'implementazione.

Procedere come descritto di seguito:

1. Nella scheda Amministrazione, fare clic su CA CMDB, Controllo della configurazione e Stati del Cambiamento gestiti.
2. Fare clic su Implementazione in corso per aprire la pagina dei dettagli dello stato gestito.
3. Verificare i dettagli dello stato gestito.

   Ad esempio, se si decide consentire la modifica delle specifiche del Cambiamento con lo stato Implementazione in corso e abilitare l'opzione Verifica del Cambiamento attiva. In questo esempio è presente un processo di verifica del Cambiamento attivo e la possibilità di modificare i valori quando l'Ordine di cambiamento è impostato sullo stato Implementazione in corso.
4. Chiudere la pagina.

Creazione di una policy di verifica per l'attributo gestito

La policy di verifica specifica l'azione CACF da eseguire quando un MDR rileva un valore di attributo e tenta di aggiornare CMDB con tale dato.

Procedere come descritto di seguito:

1. Nella scheda Amministrazione, fare clic su CA CMDB, Controllo della configurazione e Policy di verifica.
2. Fare clic su Crea Nuovo per aprire la pagina dei dettagli.
3. Immetter **1000** come valore della sequenza della policy.

   Nota: è possibile immettere un numero superiore o inferiore in base ad altre priorità della policy di verifica in uso nell'ambiente.
4. Immettere un nome di policy, ad esempio **RAM Management** e una breve descrizione della policy.
5. Selezionare Inserimento non autorizzato e Aggiornamenti non autorizzati in Allineamento Ordine di cambiamento.

6. Se si desidera impostare la policy per impedire l'aggiornamento di un attributo Memoria installata (phys_mem) da parte di un MDR specifico, completare le attività seguenti:

   - Selezionare Memoria installata come attributo gestito.
   - Immettere uno schema di ruolo oppure utilizzare un asterisco per l'applicazione a tutti i ruoli.
   - Immettere un modello di nome dell'elemento della configurazione oppure utilizzare un asterisco per l'applicazione a tutti i gli elementi della configurazione.
   - Immettere un modello di classe oppure utilizzare un asterisco per l'applicazione a tutte le classi.
   - Selezionare Mantieni il valore di attributo precedente per l'opzione Aggiorna comportamento.

   Nota: se si desidera consentire l'aggiornamento a questo attributo solo agli utenti che hanno eseguito l'accesso tramite l'interfaccia Web, immettere **client Web** come Modello di nome MDR.

7. Fare clic su Salva.
8. Chiudere la pagina.

Verifica dell'elenco delle specifiche del Cambiamento

Un Ordine di cambiamento con stato RFC desidera modificare il valore dell'attributo Memoria installata (phys_mem) in un elemento della configurazione denominato server1. Il manager del Cambiamento imposta lo stato di verifica della specifica del Cambiamento in *Richiedi verifica manuale*. Il manager del Cambiamento può visualizzare la specifica del Cambiamento in CA SDM.

Procedere come descritto di seguito:

1. Il manager del Cambiamento modifica lo stato dell'Ordine di cambiamento da RFC a Verifica in corso.

   Tutte le specifiche del Cambiamento con verifica manuale vengono convertite in Verifica manuale attiva.

2. In Ordine di cambiamento, selezionare la scheda Specifiche del Cambiamento dalla scheda Gestione della configurazione.

   La scheda evidenzia tutte le specifiche del Cambiamento in rosso per indicare che viene richiesta la verifica manuale.

   Nota: è possibile visualizzare le specifiche del Cambiamento dalla scheda Amministrazione, selezionando CA CMDB, Audit di configurazione, Specifiche del Cambiamento. Inoltre, è possibile visualizzare le specifiche del Cambiamento da un elemento della configurazione, selezionando Specifiche del Cambiamento dalla scheda Ticket correlati.

3. Individuare le specifiche del Cambiamento con stato di verifica *Richiedi verifica manuale*.

   Ad esempio, le specifiche del Cambiamento dell'Ordine di cambiamento 21 presentano tale stato.

4. Individuare il valore appropriato per l'attributo Memoria installata per l'elemento della configurazione del server1.

   Nota: le specifiche del Cambiamento che non superano la verifica vengono contrassegnate in rosso per evidenziare le specifiche del Cambiamento che richiedono un'ulteriore analisi.

Accettazione del valore pianificato

Il manager del Cambiamento individua il valore di attributo corretto per l'elemento della configurazione ed effettua le azioni necessarie per la Richiesta di cambiamento.

Procedere come descritto di seguito:

1. Aprire la specifica del Cambiamento per visualizzare la pagina dei dettagli.
2. Individuare l'attributo Memoria installata (phys_mem) per l'elemento della configurazione e confermare il valore pianificato.
3. Verificare che lo stato dell'Ordine di cambiamento della specifica del Cambiamento sia Verifica in corso.
4. Fare clic su Accetta valore pianificato.

   Lo stato Verifica in corso viene modificato in Valore pianificato accettato.

   Nota: dopo aver selezionato Accetta valore pianificato, l'elemento della configurazione esegue automaticamente l'aggiornamento del valore pianificato.

La verifica manuale del valore dell'attributo gestito viene completato correttamente.

Esempio: Autorizzazione degli aggiornamenti non autorizzati solo da una posizione specifica

In questo esempio, gli elementi della configurazione del server dell'ufficio di New York richiedono un intervento. Il vendor incaricato della riparazione dei server risiede nella stessa ubicazione. Il manager di asset richiede l'invio dei server difettosi a New York. L'amministratore della configurazione desidera consentire gli aggiornamenti non autorizzati agli elementi della configurazione quando l'hardware viene recapitato a New York. L'amministratore della configurazione crea una policy di verifica per l'attributo Vendor di manutenzione per consentire all'analista di Service desk di New York di verificare la ricezione del server da parte del vendor.

Procedere come descritto di seguito:

1. Creare l'attributo gestito seguente:
   - Immettere **vendor_repair** come nome dell'attributo.
   - Selezionare Verifica in sospesa dall'elenco a discesa Stato iniziale.
   - Immettere **Manutenzione** come etichetta e la descrizione dell'attributo gestito.
2. Creare il seguente stato del Cambiamento gestito:
   - Immettere **In sospeso (vendor)** come stato dell'Ordine di cambiamento.
   - Abilitare l'opzione Verifica del Cambiamento attiva.

3. Creare la seguente policy di verifica:
   - Selezionare Inserimento non autorizzato e Aggiornamento non autorizzato come allineamento dell'Ordine di cambiamento.
   - Immettere un numero di sequenza per la policy.

     Ad esempio, immettere **201**.
   - Immettere **server*** come nome di modello dell'elemento della configurazione.
   - Immettere **Server** come modello di classe.
   - Immettere **New York** come schema di posizione.
   - Selezionare Consenti aggiornamento dell'attributo dall'elenco a discesa Aggiorna comportamento.
4. L'Analista di Service Desk crea un Ordine di cambiamento e le specifiche del Cambiamento per gli elementi della configurazione del server e specifica New York come posizione.
5. L'analista di Service Desk imposta lo stato dell'Ordine di cambiamento su In sospeso (vendor).
6. L'analista di Service Desk aggiorna la posizione degli elementi della configurazione del server su New York.

   Ad esempio, i server difettosi dell'ufficio di Chicago vengono inviati a New York e l'analista di Service Desk verifica l'arrivo dei server a New York.
7. L'analista di Service Desk immette le informazioni del vendor nell'elemento della configurazione.

   L'Ordine di cambiamento viene chiuso in seguito all'impostazione di tutte le posizioni dell'elemento della configurazione su New York e la verifica di tutte le specifiche del Cambiamento.

Esempio: Aggiornamento dei computer portatili dell'organizzazione

In questo esempio, il manager di asset desidera eseguire l'aggiornamento di tutti i computer portatili dell'organizzazione da Windows XP a Windows 7. L'amministratore della configurazione crea una policy di verifica per l'attributo Versione del prodotto per filtrare tutti i computer portatili con sistema operativo Windows XP. L'amministratore della configurazione crea una definizione dell'attributo gestito con stato *Usa valore rilevato*, verifica gli stati gestiti e crea una policy di verifica. CA SDM riceve gli aggiornamenti in CMDB mediante CA Configuration Automation dai computer portatili che richiedono un aggiornamento del sistema operativo e il team di gestione degli asset completa l'aggiornamento.

Procedere come descritto di seguito:

1. Creare l'attributo gestito seguente:
   - Immettere **product_version** come nome dell'attributo.
   - Immettere **Versione del prodotto** come etichetta dell'attributo.
   - Selezionare Usa valore rilevato dall'elenco a discesa Stato iniziale.
   - Immettere un'etichetta e una descrizione dell'attributo gestito.
2. Creare la seguente policy di verifica:
   - Immettere una sequenza basata su altre policy dell'organizzazione.

     Ad esempio, immettere **101**.
   - Immettere **Windows* XP*** come modello di nome dell'elemento della configurazione.
   - Immettere **Workstation** come modello di classe.
   - (Facoltativo) Immettere uno schema di posizione se si desidera associare la policy con un ufficio specifico dell'organizzazione.
   - Selezionare Consenti aggiornamento solo in caso di corrispondenza con la specifica del Cambiamento dall'elenco a discesa Aggiorna comportamento.
   - Selezionare Sì nell'elenco a discesa Crea Incidente.
3. Creare un Ordine di cambiamento e le specifiche del Cambiamento indicanti Windows 7 come versione del prodotto dell'attributo gestito per ciascun elemento della configurazione del computer portatile.
4. Modificare lo stato dell'Ordine di cambiamento in Implementazione in corso e attendere l'aggiornamento da parte del team di gestione degli asset.
5. Una volta completata l'implementazione, impostare l'Ordine di cambiamento su Verifica in corso.

   CA Configuration Automation rileva le informazioni del computer portatile ed esegue l'importazione dei dati in CMDB.
6. Visualizzare l'elenco Incidenti CACF aperti per eventuali varianze rilevate da CACF.

7. Selezionare un Incidente e verificare i dettagli relativi al computer portatile rilevato da CA Configuration Automation.
8. Fare clic su Crea Ordine di cambiamento e associare l'elemento della configurazione al ticket, quindi indicare le specifiche del Cambiamento per la versione di prodotto delle modifiche principali.

   Attendere che il rilevamento verifichi tutte le modifiche restanti completetate.
9. Ripetere le fasi 6-8 per i nuovi Incidenti creati da CACF, in base alle proprie esigenze.

Esempio: Blocco degli Ordini di cambiamento non verificati

In questo esempio, l'amministratore della configurazione desidera consentire l'aggiornamento dell'elemento della configurazione unicamente per l'Ordine di cambiamento corrispondente. Viene eseguito solo l'aggiornamento degli elementi della configurazione con classe del server ubicata in NY per rilevare gli Ordini di cambiamento verificati. Qualsiasi varianza genera un Incidente.

Procedere come descritto di seguito:

1. Creare una policy di verifica.
2. Completare le fasi seguenti:
   a. Immettere un numero di sequenza.
   b. Selezionare Tutti gli attributi gestiti come attributo gestito.
   c. Immettere **NY** come schema di posizione.
   d. Immettere **Server** come modello di classe.
   e. Selezionare Consenti aggiornamento solo in caso di corrispondenza con la specifica del Cambiamento come comportamento dell'aggiornamento.
   f. Selezionare Sì nell'elenco a discesa Crea Incidente.
3. Salvare la policy.

Esempio: Autorizzazione dell'aggiornamento dell'elemento della configurazione nel caso in cui non esista un Ordine di cambiamento corrispondente

In questo esempio, l'amministratore della configurazione desidera consentire l'aggiornamento di tutti gli elementi della configurazione denominati test*, incluso nel caso in cui non sia disponibile alcun Ordine di cambiamento corrispondente. Questa policy accetta gli aggiornamenti eseguiti da tutti gli utenti con ruolo amministrativo.

Procedere come descritto di seguito:

1. Creare una policy di verifica.
2. Completare i passaggi seguenti:
   a. Immettere un numero di sequenza.
   b. Selezionare Tutti gli attributi gestiti come attributo gestito.
   c. Immettere **test*** come nome di modello dell'elemento della configurazione.
   d. Immettere **Administrator*** come schema di ruolo.
   e. Selezionare Consenti aggiornamento dell'attributo come comportamento dell'aggiornamento.
3. Salvare la policy.
4. Un utente con un ruolo amministrativo crea una specifica del Cambiamento per un elemento della configurazione denominato test5.

   L'elemento della configurazione viene aggiornato correttamente.

Esempio: Rinvio degli aggiornamenti da CA Configuration Automation all'area di lavoro della transazione

In questo esempio, l'amministratore della configurazione desidera differire tutti gli aggiornamenti dell'elemento della configurazione da CA Configuration Automation all'area di lavoro della transazione. Questa policy non esegue l'aggiornamento dell'elemento della configurazione in CMDB ed esegue la scrittura dei dati per tutti i Cambiamenti non autorizzati all'area di lavoro della transazione per una valutazione successiva.

Procedere come descritto di seguito:

1. Creare una policy di verifica.
2. Completare i passaggi seguenti:
   a. Immettere un numero di sequenza.
   b. Selezionare Tutti gli attributi gestiti come attributo gestito.
   c. Selezionare Inserimento non autorizzato e Aggiornamento non autorizzato come allineamento dell'Ordine di cambiamento.

d. Immettere **CCA** come modello di classe MDR.

e. Selezionare Annulla sempre l'intera transazione come comportamento dell'aggiornamento.

f. Selezionare Sempre per l'opzione Esegui la scrittura dei dati nell'area di lavoro della transazione.

3. Salvare la policy.

Esempio: Registrazione dei risultati della policy come test

In questo esempio, l'amministratore della configurazione desidera testare una nuova policy prima di implementarla nell'ambiente CMDB. L'opzione Solo accesso consente a CACF di eseguire la scrittura dell'impatto potenziale dell'elemento della configurazione della policy nel file di registro standard.

Procedere come descritto di seguito:

1. Creare una policy di verifica.
2. Completare le informazioni relative all'allineamento, i filtri e l'azione.
3. Selezionare l'opzione Modalità Solo accesso
4. Salvare la policy.
5. Visualizzare il file di registro standard dopo avere eseguito gli aggiornamenti dell'elemento della configurazione corrispondente alle specifiche della policy e ai criteri del filtro per simulare l'esecuzione della policy.

Esempio: Rifiuto dell'aggiornamento di un elemento della configurazione

In questo esempio, l'amministratore della configurazione desidera rifiutare gli aggiornamenti da un MDR denominato Cohesion solo per l'attributo Indirizzo IP (alarm_id). Questa policy non esegue l'aggiornamento dell'indirizzo IP dell'elemento della configurazione in CMDB, ma può aggiornare altri attributi. CACF esegue la scrittura di tutti gli attributi nell'area di lavoro della transazione per ulteriori valutazioni.

Procedere come descritto di seguito:

1. Aggiungere l'indirizzo IP (alarm_id) all'elenco degli attributi gestiti.
2. Creare una policy di verifica.
3. Completare i passaggi seguenti:

   a. Immettere un numero di sequenza.

   b. Selezionare Indirizzo IP come attributo gestito.

c. Selezionare Inserimento non autorizzato e Aggiornamento non autorizzato come allineamento dell'Ordine di cambiamento.

d. Immettere **Cohesion** come modello MDR.

e. Selezionare Mantieni il valore di attributo precedente per l'opzione Aggiorna comportamento.

f. Selezionare Sempre per l'opzione Esegui la scrittura dei dati nell'area di lavoro della transazione.

4. Salvare la policy.

Esempio: Autorizzazione di Ordini di cambiamento creati senza specifiche

In questo esempio, l'amministratore della configurazione desidera autorizzare gli Ordini di cambiamento creati dagli utenti senza specifiche. Questa policy presuppone che il testo dell'elemento della configurazione contenga la descrizione accurata di tutti i Cambiamenti e consente l'aggiornamento dell'elemento della configurazione.

Procedere come descritto di seguito:

1. Creare una policy di verifica.
2. Completare i passaggi seguenti:
   a. Immettere un numero di sequenza.
   b. Selezionare Tutti gli attributi gestiti come attributo gestito.
   c. Selezionare Ordini di cambiamento senza specifiche come allineamento.
   d. Selezionare Consenti aggiornamento dell'attributo come comportamento dell'aggiornamento.
3. Salvare la policy.

Esempio: Blocco dell'autorizzazione di Ordini di cambiamento creati senza specifiche

In questo esempio, l'amministratore della configurazione *non* desidera autorizzare gli Ordini di cambiamento creati dagli utenti senza specifiche. Questa policy ignora gli Ordini di cambiamento privi di specifiche e procede alla creazione di Incidenti.

Procedere come descritto di seguito:

1. Creare una policy di verifica.
2. Completare i passaggi seguenti:
   a. Immettere un numero di sequenza.
   b. Selezionare Tutti gli attributi gestiti come attributo gestito.

c. Selezionare Ordini di cambiamento senza specifiche come allineamento.

d. Selezionare Annulla sempre l'intera transazione come comportamento dell'aggiornamento.

e. Selezionare Sì dall'elenco a discesa Crea Incidente e selezionare un modello di Incidente.

3. Salvare la policy.

Esempio: Autorizzazione degli inserimenti non autorizzati da origini selezionate

In questo esempio, l'amministratore della configurazione desidera autorizzare nuovi elementi della configurazione da origini selezionate. Gli MDR z/OS possono creare elementi della configurazione senza richiedere un Ordine di cambiamento.

Procedere come descritto di seguito:

1. Creare una policy di verifica.
2. Completare i passaggi seguenti:
   a. Immettere un numero di sequenza.
   b. Selezionare Tutti gli attributi gestiti come attributo gestito.
   c. Selezionare Inserimento non autorizzato come allineamento.
   d. Immettere **z/OS** come modello di classe MDR.
   e. Selezionare Consenti aggiornamento dell'attributo come comportamento dell'aggiornamento.
3. Salvare la policy.

Esempio: Autorizzazione di un aggiornamento non autorizzato per un elemento della configurazione non appartenente alla produzione

In questo esempio, l'amministratore della configurazione desidera consentire gli aggiornamenti dell'attributo Indirizzo IP da Spectrum MDR, ma il nome non può iniziare con *PROD*.

Procedere come descritto di seguito:

1. Creare una policy di verifica.
2. Completare i passaggi seguenti:
   a. Immettere un numero di sequenza.
   b. Selezionare Indirizzo IP (alarm_id) come attributo gestito.

c. Selezionare Aggiornamento non autorizzato come allineamento.

d. Immettere **!PROD*** come nome di modello dell'elemento della configurazione.

e. Immettere **Spectrum** come modello di classe MDR.

f. Selezionare Consenti aggiornamento dell'attributo come comportamento dell'aggiornamento.

3. Salvare la policy.

Capitolo 17: Amministrazione degli MDR

Questo capitolo spiega come definire MDR, importare i dati, associare elementi della configurazione alla fonte, definire parametri di avvio, trasferire l'avvio all'MDR fonte e usare gli MDR per associare e visualizzare le informazioni sugli elementi della configurazione federati.

Questa sezione contiene i seguenti argomenti:

Informazioni su MDR (a pagina 767)
Utilità di avvio MDR (a pagina 769)
Definizione di un URL per avviare un MDR (a pagina 770)
Impostazione di un fornitore MDR CA APM (a pagina 772)
Avvio diretto nel contesto da CA CMDB a CA APM (a pagina 772)
Proprietà dell'elemento condiviso che supportano la federazione MDR. (a pagina 773)
MDR CA Cohesion ACM (a pagina 775)
Utilizzo di GRLoader (a pagina 779)
Convenzioni di denominazione per gli elementi della configurazione e limitazioni (a pagina 780)
Convenzione di denominazione per nome_sistema (a pagina 781)
Utilizzo di Visualizzatore CMDBf (a pagina 782)
Modalità di aggiornamento di file di metadati per la mappatura CMDBf (a pagina 783)

Informazioni su MDR

CMDBf (Configuration Management Database Federation), un gruppo di lavoro composto di rappresentanti CA, IBM, HP, Microsoft e altre aziende, ha definito un repository dei dati di gestione (MDR) come uno strumento che raccoglie informazioni relative agli elementi della configurazione.

Per creare una relazione completa fra un MDR e gli elementi della configurazione durante l'implementazione di MDR Launcher, effettuare le seguenti operazioni:

1. Definire l'MDR.
2. Definire gli elementi della configurazione che fanno riferimento all'MDR.

   Non è possibile avere un elemento della configurazione che fa riferimento a un MDR inesistente, ma è possibile definire un elemento della configurazione senza definirne l'associazione con un MDR. È possibile aggiungere le informazioni relative all'MDR durante un aggiornamento o una modifica per sfruttare la meglio le potenzialità di MDR Launcher.

Lo stesso elemento della configurazione può essere individuato da più MDR. Quando l'elemento della configurazione viene individuato, ogni MDR tenta di gestirlo. Un MDR può eseguire le azioni seguenti:

- Individuare attributi dettagliati dell'elemento della configurazione.
- Tentare di modificare lo stato dell'elemento della configurazione.

Esempio: Un elemento della configurazione individuato da più MDR

Un elemento della configurazione viene individuato da un software di gestione di rete e da un pacchetto software per la gestione di asset.

- Il software di gestione di rete gestisce le informazioni sulla configurazione e la topologia della rete.
- Il software per la gestione di asset contiene informazioni relative ai costi, all'ammortamento, ai contratti di licenza e di manutenzione per quell'elemento della configurazione.

Classi MDR e nomi MDR

È possibile che un'azienda IT includa molti MDR. Ogni MDR ha un identificatore, detto *nome MDR (nome_mdr*). Poiché è comune per un MDR l'utilizzo di un server host come *nome_mdr*, per consentire a più MDR di trovarsi sul medesimo server host, viene aggiunta una *classe MDR* (*classe_mdr*) al *nome_mdr* per consentire l'identificazione univoca dell'MDR.

CA Cohesion ACM è uno strumento aziendale che si integra perfettamente con CA CMDB. Ogni MDR CA Cohesion ACM definito in CA CMDB deve avere una *classe_mdr* **Cohesion**.

Nota: per ulteriori informazioni su CA Cohesion ACM, consultare la Guida in linea corrispondente. Per l'integrazione tra CA Cohesion ACM e CA CMDB, consultare la *Guida all'implementazione di CA Cohesion ACM*.

Come avviene l'integrazione di un MDR con CA SDM?

Un MDR contiene in genere informazioni più dettagliate sugli elementi della configurazione rispetto a CA CMDB. Tuttavia, un singolo MDR non include informazioni su altri MDR né considera le relazioni esistenti fra un elemento della configurazione e gli altri, soprattutto se tali elementi sono contenuti in altri MDR. CA CMDB è molto utile per la gestione di questo tipo di ambienti poiché si occupa della gestione degli elementi della configurazione a prescindere dall'MDR di appartenenza.

CA CMDB non archivia tutti gli attributi per gli elementi della configurazione, ma li utilizza per consolidare gli attributi di maggior importanza da gestire in modo centralizzato. Gli attribuiti controllati dalla gestione dei cambiamenti rappresentano i candidati ideali per l'inclusione in CMDB. È possibile accedere agli attributi non gestiti da CA CMDB mediante le funzionalità di MDR Launch. Inoltre, CA CMDB fornisce anche il Visualizzatore CMDBf che consente di effettuare confronti affiancati degli attributi degli elementi della configurazione tra più CMDB ed MDR.

Definizione di un MDR su CA SDM

Nella scheda Amministrazione è possibile definire un MDR su CA CMDB.

È necessario definire un MDR prima di potervi importare un elemento della configurazione. Ogni tentativo di importare un elemento della configurazione federato in un MDR inesistente non verrà eseguito.

Nota: per istruzioni sulla definizione di un MDR, consultare la *Guida all'implementazione*.

Utilità di avvio MDR

MDR Launcher è uno strumento di integrazione aperta che consente di visualizzare i dati di quasi tutti gli MDR utilizzando una pagina Web, senza dover ricorrere alla programmazione. MDR Launcher consente a chiunque visualizzi un elemento della configurazione di recuperarne dettagli aggiuntivi e di ottenere il controllo su di esso (se MDR supporta tale controllo).

Di seguito sono indicati i principali utilizzi di MDR Launcher:

- Dalla pagina dei dettagli del server hardware, avviare CA Cohesion ACM per verificare il cambiamento.
- Da un dettaglio relativo a un elemento della configurazione Aria condizionata, avviare la pagina Web di un fornitore per informazioni di diagnostica e di reporting errori.
- Da un elemento della configurazione di un contratto, avviare un sistema di gestione contratti per visualizzare le informazioni del contatto.
- Da un elemento della configurazione SLA, avviare il servizio CA per revisionare lo SLA (Service Level Agreement) prima di apportare qualsiasi modifica.
- Da un elemento della configurazione server, avviare CA Remote Control per eseguire l'analisi e l'eventuale correzione dei problemi.

Definizione di un URL per avviare un MDR

Per abilitare il funzionamento di MDR Launcher, CA CMDB utilizza un URL per avviare una sessione del browser Web con l'MDR di origine. Occorre definire l'URL utilizzato da CA CMDB.

Per definire l'URL di un MDR

1. Fare clic sulla scheda Amministrazione.
2. Nel riquadro sinistro, aprire la struttura di gestione degli MDR CA CMDB.
3. Fare clic su Elenco MDR.

   Viene visualizzata la pagina Elenco Management Data Repository.
4. Fare clic su un MDR esistente oppure crearne uno e salvarlo.

   Viene visualizzata la pagina Definizione MDR Provider.
5. Fare clic su Modifica.

   Viene visualizzata la pagina Aggiorna la definizione MDR.
6. Compilare i parametri seguenti:

   Nome host

   Consente di specificare l'indirizzo di rete o il nome DNS per il server delle pagine Web per l'MDR.

   Porta

   Consente di specificare il numero di porta utilizzato dal server Web del nome host.

Percorso

Consente di specificare il percorso della pagina Web, inclusa la pagina stessa.

Parametri

Consente di specificare qualsiasi parametro utilizzato per identificare l'elemento della configurazione desiderato per l'MDR. CA CMDB invia queste informazioni all'MDR.

Userid

Consente di specificare l'ID utente, se per l'accesso all'MDR è consentito l'utilizzo di un ID utente comune.

Segreto condiviso

Consente di specificare le informazioni condivise tra CA CMDB e l'MDR. Per gli MDR CA Cohesion, il valore specificato qui deve corrispondere a quello specificato nel file delle proprietà di CA Cohesion per il valore com.cendura.security.oneclickauth.secret.

Spazio nomi di CMDBf

Specifica il federated_asset_id che viene passato alla query come ID locale. Per CA CMDB, il valore è http://cmdb.ca.com/r1.

CMDBf Timeout

(Opzionale) Specifica il limite di tempo per query endpoint CMDBf. L'impostazione predefinita è dieci (10) secondi.

Endpoint CMDBf

Specifica l'endpoint Servizio query per MDR. Questa opzione è necessaria per il Visualizzatore CMDBf e per recuperare i dati MDR aggiornati. Se si utilizza CA CMDB come fornitore MDR, il valore sarà http://cmdb_hostname:cmdb_port/axis/services/QueryPort.

Salvare la definizione.

L'URL è stato definito.

Nota: l'URL può contenere anche le variabili di sostituzione per qualificare ulteriormente l'elemento della configurazione per l'MDR. Per ulteriori informazioni, consultare la *Guida all'implementazione*.

Impostazione di un fornitore MDR CA APM

È possibile impostare un MDR come fornitore CA APM.

Procedere come descritto di seguito:

1. Nella scheda Amministrazione, fare clic su CA CMDB, Gestione MDR e Elenco MDR.
2. Fare clic su Crea nuovo per specificare l'MDR CA APM.

   Viene visualizzata la definizione del provider MDR.

3. Immettere le seguenti informazioni obbligatorie per il provider MDR:
   - Nome pulsante—Specificare APM o qualsiasi altro nome pulsante valido. Si consiglia di utilizzare il nome pulsante APM.
   - Nome MDR—Specificare APM per CA Asset Portfolio Management r11.3.4 o ITAM per CA APM r12.6
   - Classe MDR—Specificare GLOBAL.
   - Nome host—Specificare il nome server CA APM utilizzando l'indirizzo di rete o il nome DNS del server Web CA APM.
   - URL per l'avvio nel contesto—Il valore indicato è http://{hostname}:{port}/{path}?{parameters} è non deve essere modificato.

   Il modulo del provider MDR inserisce automaticamente i valori del percorso e dei parametri con le informazioni richieste per l'avvio nel contesto CA APM.

4. Fare clic su Salva.

   Il provider MDR CA APM viene impostato.

   Nota: per ulteriori informazioni su MDR Launcher, consultare la *Guida all'implementazione*.

Avvio diretto nel contesto da CA CMDB a CA APM

La funzionalità MDR Launcher di CA CMDB supporta l'avvio diretto nel contesto da CA APM qualora CA APM e CA CMDB condividano lo stesso MDB. Se un utente crea una definizione speciale per il fornitore MDR CA APM, nell'interfaccia utente di CA CMDB compare un pulsante di avvio nel contesto nella scheda Attributi del modulo Dettagli elementi della configurazione.

La definizione MDR CA APM dispone di tutte le funzionalità di un MDR tradizionale. La funzionalità di controllo delle versioni di CA CMDB supporta anche l'avvio diretto nel contesto da una voce di registro attributo associata a ogni cambiamento CA APM.

Importante A differenza di altri MDR, l'MDR CA APM è associato automaticamente a ogni elemento della configurazione o asset. Inoltre, la classe MDR di GLOBAL e il nome MDR APM sono utilizzati per identificare l'MDR CA Asset Portfolio Management r11.3.4. Inoltre, la classe MDR di GLOBAL e il nome MDR di ITAM sono utilizzati per identificare l'MDR CA APM r12.6. L'utilizzo dell'MDR CA APM è completamente compatibile con altri MDR, anche per lo stesso elemento della configurazione.

Proprietà dell'elemento condiviso che supportano la federazione MDR.

Le proprietà (attributi) degli elementi della configurazione identificano gli asset ai fini della federazione di MDR.

ID asset federato

Le persone vengono riconosciute dalle diverse organizzazioni in base a identificatori diversi. È possibile essere riconosciuti in base ai seguenti identificatori:

- Un soprannome univoco per gli amici
- Il numero della patente di guida (ID univoco associato all'utente)
- Il numero della carta di identità
- Un numero di assicurazione
- Il codice fiscale

Ciascuno di questi identificatori è univoco della persona; tuttavia, l'identificatore è valido solo quando utilizzato per descrivere la persona all'appropriato repository.

Analogamente, un elemento della configurazione può presentare più identificatori per l'associazione con i rispettivi MDR fonte. Ciascun elemento della configurazione viene riconosciuto da un MDR solo attraverso un singolo identificatore. Questo identificatore viene denominato *ID asset federato*. Il processo di associazione di un elemento della configurazione a uno o più MDR è detto *mapping dell'elemento della configurazione*.

Il mapping si verifica quando gli elementi della configurazione vengono caricati nell'MDB in uno dei due seguenti modi:

- Definizione del mapping dell'elemento della configurazione attraverso l'utilizzo dell'interfaccia utente di amministrazione
- Caricamento degli elementi della configurazione mediante l'utilità GRLoader

Nome MDR

Il nome MDR viene utilizzato da MDR per l'identificazione in CA CMDB quando si esportano i dati utilizzando XML e GRLoader. In genere, l'MDR dispone della propria convenzione di denominazione per la modalità di identificazione; si tratta di una combinazione del nome del server host e un nome o un numero di istanza di identificazione. Dato che esiste un singolo MDR su un determinato host, il nome MDR spesso è impostato sul nome del server host. **Richiesto per il Visualizzatore CMDBf.**

Importante. Il nome MDR per la CA Asset Portfolio Management 11.3.4 corrisponde a APM, mentre il nome MDR per CA APM r12.6 corrisponde a ITAM. Benché siano supportati entrambi i prodotti, è consigliabile verificare la disponibilità dei prodotti sul sito Web supportconnect.ca.com prima di implementarli.

Classe MDR

La classe di MDR viene definita dal cliente per raggruppare gli MDR.

Nota: per la visualizzazione CMDBf, è necessaria una classe MDR di CMDBf.

Importante Il nome MDR e la classe MDR devono essere univoci all'interno della propria organizzazione.

Definizione MDR con l'installazione di CA Cohesion ACM

Gli MDR CA Cohesion ACM presentano i seguenti requisiti:

- Il nome_mdr specificato nella definizione MDR sul server CA CMDB deve corrispondere esattamente al valore dell'attributo com.cendura.installation.name nel file cendura.properties sul server CA Cohesion ACM di destinazione.
- Gli MDR CA Cohesion ACM devono disporre di una classe MDR Cohesion.
- L'MDR deve specificare il nome host e il numero di porta del server CA Cohesion ACM.

Per eseguire MDR Launcher, modificare la seguente parte del file cendura.properties:

```
# -- Configure One-Click Authentication --
com.cendura.security.oneclickauth.secret=segreto_condiviso
com.cendura.security.oneclickauth.scheme=
com.cendura.security.oneclickauth.user=id_utente
```

Importante il segreto specificato nel file cendura.properties deve corrispondere al *segreto condiviso* nella definizione MDR.

MDR Launcher effettua l'accesso utilizzando l'*id utente* specificato nel file delle proprietà ed eredita i rispettivi attributi di protezione. Per poter utilizzare funzionalità quali l'aggiornamento degli attributi degli elementi della configurazione, verificare che l'utente disponga di privilegi appropriati.

Nota: ulteriori informazioni sulla creazione di un utente e sull'impostazione di opzioni di protezione per quell'utente, consultare la *Guida all'implementazione di CA Cohesion ACM.*

MDR CA Cohesion ACM

Occorre definire gli MDR CA Cohesion ACM prima di importare i dati da un server CA Cohesion ACM. Un MDR CA Cohesion ACM deve specificare una classe MDR di Cohesion.

Esempio: Definizione dell'MDR Cohesion1

Nella seguente definizione dell'MDR Cohesion1, l'XML specifica un nome MDR cohesion_server e una classe MDR Cohesion. Questi valori sono richiesti per poter importare gli elementi della configurazione.

Nome pulsante

Cohesion1

Nome MDR

cohesion_server

Classe MDR

Cohesion

Attivare?

Attivo

Proprietario

CMDBAdmin

Descrizione

Server CA Cohesion ACM di Chicago

Nome host

cohesion_server

Porta

8090

Percorso

CAisd/html/cmdb_cohesion.html

Parametri

hostname={hostname}+port={port}+family={family}+name={name}+secret={password}+federated_asset_id={federated_asset_id}

id utente

cohesion_userid

Segreto condiviso

Chicago01

URL di avvio nel contesto

http://cmdb_hostname:8080/{path}?{parameters}

Inoltre, dato che si tratta di un server Cendura, i valori sopra riportati devono corrispondere ai valori nel file cendura.properties sul server, come mostrato nel seguente esempio:

```
com.cendura.security.oneclickauth.secret=Chicago01
com.cendura.installation.name=cohesion_server
```

È possibile modificare la sintassi URL per gestire requisiti particolari.

Modalità di associazione manuale di un MDR a un elemento della configurazione

È possibile associare manualmente MDR a un elemento della configurazione utilizzando la funzionalità di mapping dell'elemento della configurazione federato nella scheda di amministrazione di CA CMDB, nella sezione Gestione MDR della struttura.

Prima di associare un elemento della configurazione a un MDR, effettuare le seguenti operazioni:

1. Creare la definizione MDR (se non esiste).
2. Creare la definizione dell'elemento della configurazione (se non esiste).
3. Identificare l'ID asset federato univoco dell'elemento della configurazione che si desidera collegare all'MDR. Questo ID è specifico dell'MDR, pertanto non rientra nell'ambito di questo documento.

   Nota: per identificare l'ID dell'asset federato, consultare la documentazione MDR.

Importazione automatica da CA Cohesion

È possibile importare elementi della configurazione direttamente da CA Cohesion ACM eseguendo un report CA Cohesion ACM e specificando il nome host, la porta, l'ID utente e la password su un server CA CMDB. Se l'MDR è definito in CA CMDB, CA Cohesion genera automaticamente l'XML per creare elementi della configurazione e relazioni, insieme alle informazioni necessarie per eseguire l'avvio MDR su un elemento della configurazione. Il report importa automaticamente gli elementi della configurazione in CA CMDB.

Nota: per ulteriori informazioni sull'esportazione di elementi della configurazione da un CA ACM (Cohesion Application Configuration Manager), consultare la guida in linea disponibile in Rapporti, dalla scheda Modello report.

Mapping di un elemento della configurazione a un MDR

Poiché ogni MDR utilizza un federated_asset_id per identificare un elemento della configurazione, questo può essere correlato a più MDR. Un federated_asset_id non deve essere univoco in tutti gli MDR, ma deve esserlo all'interno di un MDR. Ogni MDR deve avere classe MDR e nome MDR univoci.

Importante: ogni volta che un elemento della configurazione o un provider MDR viene reso inattivo, diventano inattivi anche tutti i mapping di elementi della configurazione federati associati all'elemento della configurazione o al provider MDR.

Dopo aver creato una definizione di provider di dati MDR, effettuare le seguenti operazioni:

1. Creare in CMBD un elemento della configurazione che faccia riferimento a un MDR.
2. Verificare che la definizione MDR funzioni.

   Dato che è possibile eseguire l'avvio solo dall'interno del contesto di un elemento della configurazione, non è possibile effettuare una verifica direttamente dalla definizione MDR, che non dispone di un contesto di elemento della configurazione.

È possibile visualizzare elenco di mapping degli elementi della configurazione federati nella scheda Amministrazione, all'interno del nodo Mapping dell'elemento della configurazione federato.

Per visualizzare l'elemento della configurazione in un contesto MDR particolare, fare clic su un pulsante di avvio MDR.

L'MDR di destinazione viene avviato nel contesto dell'elemento di configurazione aperto.

Esempio: Mapping dell'elemento della configurazione

1. Fare clic sulla scheda Amministrazione.
2. Accedere a Gestione MDR, nodo Mapping dell'elemento della configurazione federato.

   Viene visualizzato l'Elenco di mapping dell'elemento della configurazione federato.
3. Immettere server1 nel campo Nome elemento della configurazione.

   Le colonne seguenti mostrano i valori:

   ID asset federato

   1000234

   1000235

   Nome CI

   server1

   server1

   Provider MDR

   Cohesion1

   Cohesion2

   Attivo

   Attivo

   Attivo

   Il provider MDR Cohesion1 è a conoscenza dell'esistenza del server1; anche il provider MDR Cohesion2 è a conoscenza dell'esistenza di server1. L'esempio seguente mostra che ciascuno ha assegnato indipendentemente al server un ID univoco.
4. Fare clic sul nome dell'elemento della configurazione server1.

   Viene visualizzata la pagina Dettagli elemento della configurazione di server1, in cui sono presenti i pulsanti di avvio denominati Cohesion1 e Cohesion2.
5. Fare clic su uno qualsiasi dei pulsanti di avvio del provider MDR.

   Vengono visualizzati ulteriori dettagli relativi all'elemento della configurazione.

Amministrazione delle definizioni MDR

L'amministrazione delle definizioni MDR è un processo flessibile. È possibile modificare i parametri in una definizione di MDR anche se esistono elementi della configurazione che vi fanno riferimento. Ad esempio, il nome pulsante, il nome host, l'ID utente, il segreto condiviso e così via possono essere tutti modificati dopo aver definito l'MDR e aver caricato gli elementi della configurazione.

Report di CA Cohesion ACM

CA ACM (Cohesion Application Configuration Manager) fornisce una funzionalità per la pianificazione di rapporti ricorrenti. È possibile utilizzare questa funzionalità per semplificare il processo di mantenimento della sincronizzazione del CMDB con i dati nell'MDR CA Cohesion ACM. Errori comuni quali una password non valida (a causa della modifica della password o della sua scadenza) possono impedire l'importazione dei dati. Per ricevere un avviso circa eventuali errori che potrebbero verificarsi durante l'importazione dei dati in background, abilitare l'opzione per la notifica nel report di esportazione di CA CMDB in CA Cohesion ACM. Verrà inviato un messaggio di posta elettronica quando si verifica un errore di importazione. Se si esegue il report Cohesion in background come operazione pianificata, si consiglia di abilitare l'opzione per la notifica.

Nota: per ulteriori informazioni sulla pianificazione dell'esecuzione periodica di un report relativo all'esportazione di CA CMDB, consultare la *guida del prodotto CA Cohesion ACM*.

Utilizzo di GRLoader

Se utilizza GRLoader per il caricamento di un elemento della configurazione, è necessario compilare i campi seguenti nel file XML per consentire l'avvio di MDR:

- <mdr_class>
- <mdr_name>
- <federated_asset_id>

I valori forniti per <mdr_name> e <mdr_class> nel file XML devono corrispondere esattamente ai valori forniti nella definizione MDR.

Importante. Per eseguire l'importazione degli elementi della configurazione referenti a MDR, il nome e la classe MDR devono essere definiti utilizzando l'interfaccia di amministrazione. Se l'MDR specificato nell'XML non viene definito, l'elemento della configurazione non viene importato.

GRLoader supporta l'importazione degli elementi della configurazione e delle relazioni degli elementi della configurazione da fogli di calcolo con formato XLS e XLSX. Per caricare dati dell'elemento della configurazione in CA SDM, è necessario formattare i dati di origine in XML o in fogli di calcolo Excel Microsoft.

Nota: per ulteriori informazioni sull'utilizzo di GRLoader per il caricamento dei dati in un foglio di calcolo, consultare la *Guida di riferimento tecnico di CA CMDB*.

Convenzioni di denominazione per gli elementi della configurazione e limitazioni

Per gli elementi della configurazione valgono le seguenti convenzioni di denominazione e le limitazioni indicate:

- Nome CI

  Si tratta di un nome comune o di un nome di visualizzazione utilizzato negli elenchi di elementi della configurazione. La lunghezza totale del nome non deve superare 255 caratteri. Non è necessario che il nome dell'elemento della configurazione sia univoco; tuttavia, si consiglia che lo sia globalmente. Inoltre, nelle situazioni in cui il nome è determinato da un MDR, si consiglia che gli amministratori di MDR creino un nome leggibile da tutti quando compilano questo campo.

- Elementi della configurazione del software

  Nel caso di software di terze parti, seguire la stessa convenzione di denominazione degli elementi della configurazione utilizzata per i nomi creati manualmente utilizzando la scheda Amministrazione. Se si utilizzano convenzioni di denominazione corrispondenti, gli elementi della configurazione individuati con CA Cohesion ACM possono essere riconciliati con quelli creati manualmente. Se questa convenzione non viene seguita, esiste la possibilità che vengano creati più elementi della configurazione anche quando esiste una sola istanza software.

- Utilizzo dell'attributo systemname

  L'attributo systemname associa in maniera univoca un *singolo* elemento della configurazione a un determinato nome host.

  Se si importano più elementi della configurazione che specificano lo stesso attributo systemname come elemento della configurazione esistente, è possibile effettuare una riconciliazione per essere certi che venga restituito un solo elemento della configurazione.

Esempio

Le righe di output seguenti mostrano la creazione di un elemento della configurazione server (provider), un elemento della configurazione software (dipendente) e una relazione *runs* (esecuzione) tra di essi. La relazione che si ottiene rappresenta un server che esegue il software Apache.

```
Elemento della configurazione:  Nome: Server1    Classe: Server   Systemname: Server1
Elemento della configurazione:  Nome: Apache1   ON Server1      Class: Software
Relazione:  Server1 su cui è in esecuzione Apache1   ON Server1
```

Convenzione di denominazione per nome_sistema

Si consiglia di seguire gli standard di denominazione seguenti per gli elementi della configurazione software e tutti gli MDR, in modo che altri MDR possano integrarsi in modo adeguato con CA Cohesion ACM e tra di essi e anche per garantire che gli elementi della configurazione vengano riconciliati correttamente. CA Cohesion ACM segue gli stessi standard.

Nome_sistema

Consente di identificare gli elementi della configurazione software in maniera univoca. Quando si definisce una relazione che coinvolge un elemento della configurazione software, specificare lo stesso nome_sistema indicato nella definizione di elemento della configurazione. Se nella directory sullo stesso nome host sono presenti istanze multiple del medesimo software, modificare il nome_sistema in modo che sia univoco. Per il nome_sistema è consentito il numero massimo di 255 caratteri; se la limitazione non viene rispettata i caratteri potrebbero venire visualizzati in maniera errata.

Nome_sistema deve essere un identificatore univoco per l'istanza del software su un singolo host.

Utilizzare la seguente sintassi:

nome host | nome software | versione | applicazione-business

simbolo (|)

Separa i vari campi nella concatenazione della sintassi per consentire all'utente di utilizzare la funzionalità di ricerca.

nome host

Consente di specificare il nome dell'host su cui è contenuto il software.

nome software

Consente di specificare un nome comune per il software.

versione

Consente di specificare il numero di versione del software se è disponibile.

applicazione-business

Consente di specificare un identificatore univoco per l'istanza del software presente sul *nome host.* Se l'istanza del software è associata a un'applicazione aziendale o a un servizio, il qualificatore deve essere il nome di quel servizio. Se non è possibile determinare l'*applicazione-aziendale*, è possibile utilizzare la directory di installazione per identificare il software. Se la lunghezza totale di questo campo supera i 255 caratteri, utilizzare i puntini sospensivi (...) per abbreviare la lunghezza totale del campo a un numero di caratteri non superiore a 255.

Esempio: Utilizzo della funzionalità di ricerca nell'interfaccia utente

È possibile utilizzare tale funzionalità per cercare elementi della configurazione software, come illustrato negli esempi indicati:

Caso di utilizzo	Nome	Nome_sistema
Trova tutte le istanze degli elementi della configurazione sull'host	xxx	Xxx
Trova tutte le istanze del software	yyy	yyy%
Trova tutte le istanze del software	yyy versione 123.0	yyy% %|%|123.0%

Nell'elenco di risultati restituiti dalla ricerca precedente, l'utente visualizza solo il campo "nome".

```
mac_address    Null.  - Non appropriato per il software
asset_num      Null   - Non appropriato per il software
serial_number  Null   - Non appropriato per il software
dns_name       Null   - Non appropriato per il software
```

Utilizzo di Visualizzatore CMDBf

In CA SDM è disponibile il Visualizzatore CMDBf che consente di visualizzare i risultati della federazione di elementi della configurazione nei repository dati di gestione MDR. Da una pagina Dettagli elemento della configurazione (oppure nel menu di scelta rapida visualizzato facendo clic con il pulsante destro del mouse su un elemento della configurazione in un elenco di elementi della configurazione), fare clic su Visualizzatore CMDBf per visualizzare contemporaneamente gli attributi elemento della configurazione di CMDB federati e MDR. Nella vista federata è possibile fare clic sul pulsante Recupera per aggiornare le informazioni da qualsiasi MDR federato. Per una migliore leggibilità, i file metadata CA CMDB possono riconciliare i nomi di attributi MDR e i nomi di attributi CA CMDB.

Nota: questa funzionalità richiede repository dati di gestione MDR che supportano Query. Per configurare i risultati nella vista federata, è necessario configurare gli endpoint CMDBf MDR. Per ulteriori informazioni, consultare la *Guida all'implementazione*.

Se l'elemento della configurazione non dispone di dati federati, il visualizzatore mostra solo attributi CA CMDB.

Modalità di aggiornamento di file di metadati per la mappatura CMDBf

Per migliorare la leggibilità dei confronti tra gli attributi, è possibile usare file di metadati CA CMDB per convertire i nomi degli attributi MDR nei nomi degli attributi CA CMDB. La visualizzazione federata mostra il nome dell'attributo inviato da MDR per qualsiasi attributo sprovvisto di mapping CA CMDB. È possibile definire metadati per i fornitori di dati CMDBf allo scopo di effettuare le seguenti operazioni:

- Visualizzare i valori degli attributi MDR utilizzando i nomi degli attributi CA CMDB
- Non consentire la visualizzazione degli attributi del fornitore MDR nella visualizzazione federata
- Definire attributi del fornitore MDR che non hanno equivalenti CA CMDB

È possibile definire i metadati utilizzando il file cmdb_metadata_federation_viewer_site_attr.htmpl. Questo file contiene le istruzioni per eseguire l'aggiornamento del file. I metadati possono essere applicati a tutte le famiglie CMDB (attributi comuni) o agli attributi specifici per famiglia.

Per effettuare il mapping dei nomi degli attributi MDR esterni alle etichette CA CMDB, è necessario aggiornare il modulo cmdb_metadata_*extensiontable*.htmpl corrispondente utilizzando i seguenti campi nella macro cmdbmetadata:

- mdr_attr - nome dell'attributo MDR da convertire
- mdr_name - nome dell'MDR che viene convertito. L'uso di espressioni regolari è supportato.

Esempio: mapping degli attributi

Le seguenti tre istruzioni metadati definiscono i metadati che fanno corrispondere l'attributo CA CMDB "phys_mem" all'attributo del fornitore "mdr_memory" per tutti i fornitori denominati "myMdr" o il cui nome inizia con "MDR". Inoltre, "physical_memory" viene fatto corrispondere a "phys_mem" per tutti gli altri fornitori.

```
<macro name=cmdbMetadata attr="phys_mem" provider_attr="mdr_memory"
provider_name="myMdr">
<macro name=cmdbMetadata attr="phys_mem" provider_attr="mdr_memory"
provider_name_regexp=”MDR.*">
<macro name=cmdbMetadata attr="phys_mem" provider_attr="physical_memory"
provider_name_regexp=”.*">
```

Esempio: disattivazione della visualizzazione degli attributi

La seguente istruzione metadati nasconde l'attributo "widget_cost" del fornitore MDR per tutti i fornitori denominati "myMdr".

<macro name=cmdbMetadata hide_provider_attr="YES" provider_attr="widget_cost" provider_name="myMdr">

Esempio: impostazione di un'etichetta per un attributo

La seguente istruzione metadati consente di definire un nome attributo "ext_mem_capacity" utilizzando l'etichetta "Capacità memoria esterna" sotto alla categoria degli attributi del visualizzatore CMDBf.

```
<macro name=cmdbMetadata attr="ext_mem_capacity" category="Attributes"
heading="External Memory Capacity" help="Total external memory">
```

Ulteriori informazioni:

Modalità di visualizzazione di valori di attributo MDR con nomi di attributo CA CMDB (a pagina 784)
Come nascondere attributi di fornitore MDR (a pagina 785)
Definizione degli attributi MDR senza equivalenti CA CMDB (a pagina 786)
Definizione di metadati del fornitore di dati CMDBf (a pagina 786)

Modalità di visualizzazione di valori di attributo MDR con nomi di attributo CA CMDB

I metadati permettono di creare un'associazione tra gli attributi del fornitori MDR e gli attributi CA CMDB in modo che vengano visualizzati insieme e permettano agli utenti di vedere le differenze e condividere le etichette. Per impostazione predefinita, gli attributi MDR senza mapping, vengono visualizzati come **non in CMDB** nel visualizzatore.

Gli argomenti macro cmdbMetadata che consentono di ottenere una corrispondenza con un attributo <cmbd> con un attributo Fornitore MDR comprendono:

- attr – nome di attributo CA CMDB
- provider_attr – nome di attributo del fornitore MDR
- provider_name – nome del fornitore MDR
- provider_name_regexp – espressione regolare del nome del fornitore MDR

provider_name o provider_name_regexp sono obbligatori.

Esempio: associazione degli attributi MDR con i nomi degli attributi CA CMDB

Le seguenti tre istruzioni metadati eseguono le azioni descritte:

- Creano una corrispondenza tra l'attributo CA CMDB "phys_mem" e l'attributo del fornitore "mdr_memory" per tutti i fornitori chiamati "myMdr".
- Creano una corrispondenza tra l'attributo CA CMDB "phys_mem" e l'attributo del fornitore "mdr_memory" per tutti i nomi di fornitori che iniziano con "MDR".
- Creano una corrispondenza tra "physical_memory" e "phys_mem" per tutti gli altri fornitori.

```
<macro name=cmdbMetadata attr="phys_mem" provider_attr="mdr_memory"
provider_name="myMdr">
<macro name=cmdbMetadata attr="phys_mem" provider_attr="mdr_memory"
provider_name_regexp="MDR.*">
<macro name=cmdbMetadata attr="phys_mem" provider_attr="mdr_memory"
provider_name_regexp="MDR.*">
```

Come nascondere attributi di fornitore MDR

Alcuni attributi del fornitore MDR non devono essere visualizzati nella vista federata. È possibile nascondere i metadati di un fornitore MDR per un fornitore MDR specifico. Questa opzione può essere utilizzata solo per gli attributi del fornitore MDR, ma non si applica agli attributi <cmdb.

Gli argomenti macro cmdbMetadata utilizzabili per nascondere un attributo del fornitore includono:

- hide_provider_attr – "YES" – nasconde l'attributo del fornitore MDR
- provider_attr – nome di attributo del fornitore MDR
- provider_name – nome del fornitore MDR
- provider_name_regexp – espressione regolare del nome del fornitore MDR

provider_name o provider_name_regexp sono obbligatori.

Esempio: disattivazione della visualizzazione del solo attributo MDR

La seguente istruzione metadati permette di nascondere l'attributo "widget_cost" del fornitore MDR per tutti i fornitori denominati "myMdr".

```
<macro name=cmdbMetadata hide_provider_attr="YES" provider_attr="widget_cost"
provider_name="myMdr">
```

Definizione degli attributi MDR senza equivalenti CA CMDB

È possibile definire etichette e testo di aiuto per gli attributi del fornitore MDR che non corrispondono agli attributi CA CMDB. Questi attributi vengono visualizzati come Non in famiglia nella vista federata.

Gli argomenti macro cmdbMetadata utilizzabili per definire un attributo del fornitore includono:

- attr – nome di attributo CA CMDB
- category - nome della categoria in cui viene visualizzato l'attributo
- heading - etichetta di intestazione dell'attributo
- help - breve descrizione dell'attributo

Esempio: definizione di un attributo solo MDR

La seguente istruzione metadati consente di definire un nome attributo "ext_mem_capacity" utilizzando l'etichetta "Capacità memoria esterna" nella categoria Attributi della vista federata .

```
<macro name=cmdbMetadata attr="ext_mem_capacity" category="Attributes"
heading="External Memory Capacity" help="Total external memory">
```

Definizione di metadati del fornitore di dati CMDBf

È possibile specificare la modalità di visualizzazione dei dati nella vista federata.

Per definire i metadati per il visualizzatore CMDBf:

1. Usare Web Screen Painter per aprire il file cmdb_metadata_federation_viewer_site_attr.htmpl.
2. Determinare le modifiche che devono essere apportate ai metadati.

   Nota: il file contiene alcuni modelli di esempio.
3. Copiare il modello appropriato e sostituire gli argomenti necessari seguendo le istruzioni fornite nel file.
4. Salvare e pubblicare le modifiche.

Capitolo 18: Gestione delle modifiche

Questa sezione contiene i seguenti argomenti:

Gestione Cambiamento di CA SDM (a pagina 787)
Componenti di Gestione cambiamento (a pagina 788)
Visualizzazione del calendario dei Cambiamenti (a pagina 789)
Responsabilità del gruppo CAB (a pagina 790)
Responsabilità di Gestione cambiamenti (a pagina 792)
Definizione delle attività per il ruolo Gestione cambiamenti (a pagina 793)
Categorie di cambiamento, stato e livelli di rischio (a pagina 794)
Visualizzazione del contatore degli ordini di cambiamento (a pagina 795)
Definizione di una query memorizzata per ordini di cambiamento (a pagina 796)
Configurazione delle opzioni di Gestione cambiamenti (a pagina 797)
Calendario dei Cambiamenti (a pagina 798)
Modalità di pianificazione degli Ordini di cambiamento (a pagina 811)
Modalità di pianificazione delle finestre di cambiamento (a pagina 816)
Analisi e rilevamento dei conflitti (a pagina 820)
Visualizzazione di CA Workflow (a pagina 821)
Definizione del processo Gestione Cambiamento per CA Workflow (a pagina 823)
Console CAB e reporting (a pagina 846)
Valutazione dei rischi (a pagina 852)
Impact Explorer (a pagina 855)

Gestione Cambiamento di CA SDM

Gestione Cambiamento di CA SDM comprende una serie di funzionalità per gestori dei cambiamenti, coordinatori dei cambiamenti e membri del gruppo CAB (Change Advisory Board) al fine di coordinare la revisione e l'approvazione delle richieste di cambiamento per componenti e servizi degli elementi della configurazione. Ad esempio, i gestori dei cambiamenti possono analizzare e approvare tutti i cambiamenti effettuati su componenti e servizi degli elementi della configurazione per assicurare che non vengano introdotte nuove vulnerabilità alla sicurezza nell'ambiente di produzione. Gestione cambiamenti è a capo del gruppo CAB ed è responsabile dell'approvazione finale delle richieste di cambiamento.

Gestione cambiamenti consente di effettuare quanto segue:

- Seguire i processi ITIL, mettendo in relazione i cambiamenti alla struttura IT con la gestione degli incidenti o dei problemi.

- Visualizzare le informazioni sulla gestione dei servizi per un elemento della configurazione, come il numero di cambiamenti registrati per uno di essi, le date di implementazione dei cambiamenti e altro ancora.
- Rilevare possibili conflitti se più ordini di cambiamento richiedono la modifica degli stessi elementi della configurazione nello stesso momento.
- Creare e memorizzare finestre di cambiamento nel calendario dei cambiamenti.
- Creare un ordine di cambiamento in una visualizzazione calendario.
- Valutare i rischi associati a una modifica.

Nota: per ulteriori informazioni su come eseguire queste e altre procedure di gestione dei cambiamenti, consultare le informazioni su Gestione Cambiamento nella *Guida in linea*.

Componenti di Gestione cambiamento

Gestione cambiamento include i seguenti componenti:

Calendario dei Cambiamenti

Fornisce una visualizzazione grafica degli eventi di cambiamento (a pagina 798), incluse tutte le richieste di cambiamento pianificate, non riuscite e in corso relative a elementi della configurazione e servizi in una visualizzazione calendario (a pagina 811) configurabile. Il calendario mostra anche le date di blackout, che indicano periodi di blocco delle attività. Gli utenti possono creare un ordine di cambiamento dal menu di scelta rapida nella visualizzazione calendario giornaliera, settimanale e mensile. Questa funzione è utilizzata da Gestione cambiamenti, dagli analisti di livello 2 e membri del gruppo CAB.

Utilità di pianificazione dei cambiamenti

Visualizza periodi pianificati (a pagina 817) durante i quali possono o non possono verificarsi cambiamenti degli elementi della configurazione nel calendario dei cambiamenti. Gestione cambiamento utilizza questa funzionalità per visualizzare e creare pianificazioni di cambiamenti e associazioni di elementi della configurazione durante il periodo.

Analisi e rivelamento dei conflitti

L'analisi degli ordini di cambiamento è utile per identificare possibili conflitti di implementazione che potrebbero aumentare il rischio di errori. Questa funzionalità è utilizzata da Gestione cambiamenti.

Visualizzazione del flusso di lavoro

Mostra il processo di approvazione per le richieste di cambiamento. Questa funzionalità è utilizzata da Gestione cambiamenti.

Console CAB e reporting

Mostra una dashboard (a pagina 846) che semplifica e velocizza l'approvazione online di ordini di cambiamento che richiedono l'approvazione CAB.

In CA SDM, Gestione cambiamenti può generare un report con i dettagli sulle richieste proposte per cambiamenti pronti per essere analizzati dal gruppo CAB, oltre a distribuire elettronicamente i report a tutti i membri del gruppo CAB.

Nota: gli utenti con privilegi appropriati possono visualizzare report predefiniti relativi a conformità, previsioni, tendenze e volume hanno predefinito dei report per la gestione dei cambiamenti in BusinessObjects InfoView mediante CA Business Intelligence.

Valutazione dei rischi

Consente di allegare le valutazioni dei rischi per ogni richiesta di cambiamento inviata. L'opzione Indagine di rischio permette di creare indagini per valutare i rischi e associarle alle categorie di cambiamento. L'indagine dei rischi elenca una serie di domande a scelta multipla o singola.

Impact Explorer

Visualizza le relazioni tra gli elementi della configurazione associati a un ordine di cambiamento. Impact Explorer viene avviato dalla pagina Dettagli ordine di cambiamento per semplificare l'analisi dell'impatto (a pagina 855) su richiesta. Questa funzionalità è utilizzata da Gestione cambiamenti.

Verifica del Cambiamento

Verifica l'esecuzione accurata dei Cambiamenti e che non vengano eseguiti Cambiamenti non autorizzati. In tal modo CMDB conterrà una rappresentazione accurata e aggiornata di tutti gli elementi della configurazione gestiti.

Visualizzazione del calendario dei Cambiamenti

CA SDM consente di utilizzare varie funzioni di gestione dei cambiamenti (conformi agli standard ITIL e COBIT) per visualizzare o creare ordini di cambiamento dopo aver selezionato un *calendario dei cambiamenti*. I nuovi ordini di cambiamento vengono pianificati automaticamente per il giorno selezionato.

Il calendario dei cambiamenti riporta conflitti, mancate corrispondenze e rischi potenziali tra le pianificazioni delle modifiche, gli ordini di cambiamento e gli elementi della configurazione. È possibile utilizzare il calendario per comprendere i cambiamenti che avverranno, il loro impatto potenziale sull'ambiente IT e altro ancora.

Per visualizzare il calendario dei cambiamenti

1. Fare clic sulla scheda Calendario cambiamento.

   Vengono visualizzati i campi Filtro calendario cambiamento.

2. Compilare i campi di ricerca per visualizzare un calendario con la pianificazione relativa agli ordini di cambiamento desiderati.
3. Fare clic su Cerca.

   Nel calendario dell'ordine di cambiamento sono visualizzate informazioni che corrispondono ai criteri di ricerca.

Responsabilità del gruppo CAB

Il gruppo CAB (Change Advisory Board) coordina la revisione e l'approvazione o il rifiuto delle richieste di cambiamento per componenti e servizi di elementi della configurazione. I membri del gruppo CAB sono responsabili di quanto segue:

- Analizzare tutti i cambiamenti più importanti ai sistemi di produzione.
- Partecipare a tutte le riunioni del gruppo CAB, secondo quanto deciso da Gestione cambiamenti.
- Analizzare tutte le richieste di cambiamento inviate per determinare l'impatto, le risorse richieste per implementarli ed eventuali costi.
- Partecipare alla pianificazione e alla coordinazione del calendario dei cambiamenti.
- Fare in modo che a tutti i cambiamenti vengano assegnate valutazioni e priorità adeguate.
- Partecipare alle revisioni al termine dell'installazione.

Ulteriori informazioni:

Modalità di funzionamento del processo CAB (a pagina 791)
Assegnazione dei membri al gruppo CAB (a pagina 791)

Modalità di funzionamento del processo CAB

Il gruppo CAB è responsabile per l'analisi di tutti i cambiamenti più importanti ai sistemi di produzione. I membri del gruppo CAB vengono avvisati quando una richiesta di cambiamento richiede la loro approvazione ed eseguono le operazioni seguenti:

1. Elencano le richieste di cambiamento che devono essere analizzate dal gruppo CAB.
2. Aprono la console CAB e visualizzano le informazioni contenute nella richiesta.
3. Visualizzano la motivazione di business, il piano di implementazione, gli elementi della configurazione e la documentazione di supporto associata alla richiesta, quindi decidono se approvarla o rifiutarla.
4. Approvano o rifiutano l'ordine di cambiamento, e quello successivo nell'elenco viene visualizzato automaticamente.

   La persona che richiede il cambiamento viene avvisata automaticamente circa l'aggiornamento dello stato CAB per la richiesta di cambiamento.

Ulteriori informazioni:

Responsabilità del gruppo CAB (a pagina 790)

Assegnazione dei membri al gruppo CAB

Nella pagina Aggiornamento membri è possibile assegnare i membri a un gruppo CAB.

Per assegnare i membri al gruppo CAB

1. Selezionare la scheda Membri nella pagina Dettagli gruppo.
2. Fare clic su Aggiorna membri.

   Viene visualizzata la pagina Ricerca contatto.
3. Immettere i criteri di ricerca per visualizzare i contatti desiderati e fare clic su Cerca.

   Viene visualizzata la pagina Aggiornamento membri, che elenca i contatti corrispondenti ai criteri di ricerca.
4. Scegliere dall'elenco di sinistra i contatti da assegnare al gruppo. Per selezionare più elementi, tenere premuto il tasto Ctrl mentre si fa clic con il pulsante sinistro del mouse.

5. Una volta selezionati tutti i contatti desiderati, fare clic sul pulsante di selezione (>>).

   I contatti selezionati vengono spostati nell'elenco Membri sulla destra.

6. Fare clic su OK.

   Viene visualizzata la pagina Dettagli gruppo. I contatti selezionati sono elencati nella scheda Membri.

Responsabilità di Gestione cambiamenti

Gestione Cambiamento è responsabile del processo di gestione dei Cambiamenti a livello aziendale e dell'approvazione finale degli Ordini di cambiamento. Oltre a occuparsi di generare report di analisi delle metriche per la gestione dei cambiamenti, svolge le seguenti attività:

- Analizza le richieste di cambiamento e aggiunge stakeholder e revisori appropriati a seconda dei casi.
- Contribuisce alla risoluzione delle Issue, ad esempio rilevando possibili conflitti, anche di pianificazione, nel calendario.
- Analizza l'installazione e i piani di inattività e fallback per garantire l'accesso facilitato e la stabilità del sistema.
- Comprende i rischi di ogni cambiamento e assegna il livello di rischio appropriato.
- Controlla i cambiamenti alle varie aree per assicurarsi che siano conformi ai requisiti di gestione dei cambiamenti alle tecnologie.
- Rappresenta la propria area e comunica l'impatto dei cambiamenti con rischi elevati in occasione degli incontri settimanali del gruppo CAB.
- Supporta la fase di revisione al termine dell'installazione, in caso di problemi o cambiamenti non riusciti.
- Funge da riferimento per l'escalation da parte di richiedenti di cambiamenti, stakeholder, revisori, implementatori e gruppi di supporto.

Ulteriori informazioni:

Funzionamento del ruolo Gestione cambiamenti (a pagina 793)

Funzionamento del ruolo Gestione cambiamenti

Il ruolo Gestione cambiamento ha la responsabilità di monitorare gli ordini di cambiamento relativi all'ambiente operativo per assicurare che i componenti del team operativo rispettino le policy e i processi di business. Il calendario dei cambiamenti può facilitare la risoluzione di problemi, quali eventuali conflitti fra ordini di cambiamento, consentendo di pianificare date di blackout e periodi di blocco delle attività durante i quali è possibile modificare un elemento della configurazione o un insieme di elementi della configurazione. Il ruolo Gestione cambiamento esegue inoltre le seguenti attività:

1. Supervisiona il funzionamento della console CAB, dalla quale vengono gestite le approvazioni rapide e in linea di ordini e richieste di cambiamento.
2. Organizza i gruppi CAB con i membri appropriati per gli ordini di cambiamento presi in considerazione e organizza riunioni periodiche del gruppo CAB per analizzare i nuovi ordini di cambiamento.
3. Crea report con dettagli sulle richieste proposte per i cambiamenti pronti a essere analizzati dal gruppo CAB e distribuisce elettronicamente i report a tutti i membri del gruppo CAB.
4. Esegue un'analisi in tempo reale di ogni richiesta di cambiamento e aggiorna il record con la decisione presa durante le riunioni del gruppo CAB.
5. Utilizza BusinessObjects InfoView per gestire i report su conformità, previsioni, tendenze e volume e crea report su richiesta.
6. Rappresenta la propria area e comunica l'impatto dei cambiamenti con rischi elevati in occasione degli incontri del gruppo CAB.
7. Valuta i rischi di ogni cambiamento e garantisce che a ogni cambiamento venga assegnato il livello di rischio appropriato.

Definizione delle attività per il ruolo Gestione cambiamenti

È possibile definire le attività per il ruolo Gestione cambiamenti.

Per definire le attività per il ruolo Gestione cambiamenti

1. Nella scheda Amministrazione, selezionare Gestione protezione e ruoli, Gestione ruoli, Elenco ruoli.

   Viene visualizzata la pagina Elenco ruoli.

2. Selezionare il ruolo Gestione cambiamenti.

   Viene visualizzata la pagina Change Manager Role Detail.

3. Fare clic su Modifica.

   Viene visualizzata la pagina Aggiorna ruolo Gestione cambiamenti.

4. Per configurare le attività e le autorizzazioni di accesso per il ruolo Gestione cambiamento, utilizzare le schede e i campi seguenti:
   - Autorizzazione
   - Accesso alle funzioni
   - Interfaccia Web
   - Gestione della conoscenza
   - Visibilità documento SC
   - Schede
   - Moduli Web report
   - Risorse di accesso rapido
   - Accesso in lettura titolare
   - Accesso in scrittura titolare
5. Fare clic su Salva e chiudere la finestra.

   Il record del ruolo Gestione cambiamenti viene aggiornato.

Nota: per ulteriori informazioni sulle schede visualizzate nella pagina Dettagli ruolo Gestione cambiamento, vedere le informazioni sulla gestione dei ruoli nella *Guida in linea*.

Categorie di cambiamento, stato e livelli di rischio

È possibile definire il comportamento degli ordini di cambiamento all'interno dell'ambiente di servizio. È possibile modificare i valori predefiniti che sono installati in CA SDM oppure definirne altri.

Per gestire i valori predefiniti degli ordini di cambiamento

1. Selezionare Service Desk, Ordini di cambiamento nella scheda Amministrazione.

2. Espandere il nodo Ordine di cambiamento e selezionare *uno* dei seguenti elementi:
   - Categorie
   - Tipi di cambiamento
   - Codici di chiusura
   - Stato conflitto
   - Livello di rischio
   - Indagine di rischio
   - Stato
   - Cod stato att flusso lavoro
   - Tipi att flusso lavoro

   Viene visualizzata la pagina Elenco per l'elemento selezionato.
3. Selezionare l'elemento da modificare.

   Viene visualizzata la pagina Update Details.
4. Utilizzare i controlli disponibili nelle schede in fondo alla pagina per definire il comportamento degli ordini di cambiamento nell'ambiente.
5. Fare clic su Salva e chiudere la finestra.

   L'elemento aggiornato compare nell'elenco.

Visualizzazione del contatore degli ordini di cambiamento

Il contatore degli ordini di cambiamento mostra ordini di cambiamento, attività pianificate e conflitti assegnati ad analisti di livello 2, gestori dei cambiamenti, coordinatori dei cambiamenti o membri del gruppo CAB. È possibile anche visualizzare i record, assegnati e non, in ordine di priorità.

Per visualizzare il contatore degli ordini di cambiamento

1. Accedere a Ordini di cambiamento all'interno del contatore CA SDM.
2. Espandere le cartelle per visualizzare le cartelle nidificate per quanto segue:
   - Elementi aperti o chiusi assegnati o non assegnati
   - Conflitti risolti o non risolti
   - Attività pianificate che iniziano oggi o la prossima settimana.
3. Selezionare la cartella degli elementi che si desidera visualizzare.

   Viene visualizzata la pagina Elenco.
4. (Facoltativo) Fare clic su Mostra filtro e compilare uno o più campi specificando i criteri di ricerca desiderati per limitare l'elenco ai commenti desiderati.

5. Fare clic su Cerca.

   La pagina Elenco mostra i riepiloghi degli elementi che corrispondono ai criteri di ricerca.

6. (Facoltativo) Fare clic sul pulsante Modifica in elenco per visualizzare alcuni campi aggiuntivi che è possibile associare a un elemento.

Definizione di una query memorizzata per ordini di cambiamento

La definizione delle query memorizzate disponibili agli utenti nel contatore degli ordini di cambiamento è un'attività amministrativa. È possibile modificare le query memorizzate predefinite che sono installate in CA SDM oppure definirne altre.

Per definire una query memorizzata per ordini di cambiamento

1. Selezionare Service Desk, Dati applicazioni, Query memorizzate nella scheda Amministrazione.

   Viene visualizzato l'Elenco query memorizzate.

2. Selezionare la query memorizzata che si desidera modificare.

   Viene visualizzata la pagina Dettagli query memorizzata.

3. Fare clic su Modifica.

   Viene visualizzata la pagina Aggiorna query memorizzata.

4. Modificare i valori dei campi in modo appropriato.

5. Fare clic su Salva e chiudere la finestra.

   La query memorizzata aggiornata compare nell'Elenco query memorizzate.

Esempio: definizione di una query memorizzata per elencare gli ordini di cambiamento assegnati a un gruppo CAB a cui appartiene l'utente che ha effettuato l'accesso

Questo esempio dimostra come creare una query memorizzata per elencare solo gli ordini di cambiamento assegnati a un gruppo CAB a cui appartiene l'utente che ha effettuato l'accesso.

Per creare una query memorizzata

1. Dal contatore, accedere alla pagina Aggiorna query memorizzata.

2. Modificare i valori dei campi come segue:

   a. Selezionare Utilizzo contatore.

   b. Impostare Tipo su Ordine di cambiamento.

c. Immettere la clausola Where:

```
cab.[group]group_list.member IN (@cnt.id) AND active = 1
```

3. Fare clic su Salva e chiudere la finestra.

   La query memorizzata compare nell'Elenco query memorizzate.

Ulteriori informazioni:

Console CAB e reporting (a pagina 846)

Configurazione delle opzioni di Gestione cambiamenti

È possibile configurare le opzioni per il ruolo Gestione cambiamenti.

Per configurare le opzioni di Gestione cambiamenti

1. Selezionare Gestione opzioni nella scheda Amministrazione.
2. Espandere il nodo Gestione ordini di cambiamento.

   Viene visualizzato l'Elenco opzioni.

3. Fare clic con il pulsante destro del mouse sull'opzione desiderata e selezionare Modifica dal menu di scelta rapida.

   Viene visualizzata la pagina Update Option.

4. Modificare l'opzione in modo appropriato.
5. Fare clic su Salva e chiudere la finestra.

   L'opzione aggiornata compare nell'elenco Opzioni.

Calendario dei Cambiamenti

Modifica calendario fornisce una visualizzazione grafica degli eventi di Cambiamento, con le rispettive ore di inizio e di fine dell'implementazione. Questa visualizzazione di calendario della pianificazione dei Cambiamenti fornisce agli analisti e ai manager un sistema rapido per determinare quando si verificano gli eventi e in che modo influenzano l'ambiente, l'organizzazione e le risorse.

Il calendario consente di creare Ordini di cambiamento dalla visualizzazione giornaliera, settimanale e mensile nonché di visualizzare le finestre di Cambiamenti globali per gli Ordini di cambiamento pianificati. Se in un mese esistono più finestre di cambiamenti, vengono raggruppate come singolo gruppo di finestre di blackout. Espandere una visualizzazione settimanale o giornaliera o visualizzare le informazioni a comparsa per controllare i dettagli delle singole finestre.

Nota: è possibile unicamente esportare (a pagina 800) le pianificazioni dell'Ordine di cambiamento e non le finestre dei Cambiamenti.

Ulteriori informazioni:

Aggiunta delle informazioni di pianificazione ad un ordine di cambiamento (a pagina 798)
Modelli eventi iCalendar (a pagina 799)
Esportazione delle pianificazioni in iCalendar (a pagina 800)
Visualizzazioni di pianificazione (a pagina 801)
Configurazione della visualizzazione di pianificazione (a pagina 803)

Aggiunta delle informazioni di pianificazione ad un ordine di cambiamento

È possibile aggiungere informazioni di pianificazione quando si crea o modifica un ordine di cambiamento.

Per aggiungere le informazioni di pianificazione

1. Eseguire una delle seguenti operazioni:
   - Fare clic su File, Nuovo ordine di cambiamento.
   - Aprire un ordine di cambiamento e fare clic su Modifica.

2. Completare i seguenti campi di pianificazione:

   Tipo

   Specifica il tipo di modifica ITIL come Standard, Normale o Emergenza. È possibile definire un valore predefinito per una categoria cambiamento utilizzata da CA SDM per inizializzare i nuovi ordini di cambiamento della categoria.

   Pianifica data di inizio

   Specifica la data di inizio dell'ordine di cambiamento.

   Durata

   Specifica la durata dell'ordine di cambiamento nel formato 00:00:00.

   La pianificazione contiene solo gli ordini di cambiamento con una durata e una data di inizio della pianificazione non vuote. Il campo Tipo risulta utile per raggruppare gli ordini di cambiamento nella pianificazione, ma non influenza direttamente la pianificazione.

3. Continuare a creare l'ordine di cambiamento.
4. Al termine, fare clic su Salva.

   Le informazioni di pianificazione vengono aggiunte all'ordine di cambiamento.

Modelli eventi iCalendar

I modelli eventi iCalendar controllano le informazioni esportate nel formato iCalendar.

In CA SDM sono installati i seguenti modelli predefiniti:

- Modifica pianificazione
- KnowledgeScheduleCreation
- KnowledgeScheduleExpired
- KnowledgeScheduleReview
- KnowledgeScheduleStart

Nota: è possibile modificare i codici dei modelli eventi iCalendar predefiniti ma non eliminarli o crearne di nuovi.

Importante La variabile SchedExpMaximum in web.cfg controlla il numero massimo di eventi consentiti in un'esportazione. Incrementare il valore predefinito (1 000) può causare instabilità di sistema. Se si tenta di esportare un numero maggiore di eventi rispetto al valore specificato in SchedExpMaximum, viene visualizzato un messaggio che informa dell'impossibilità di eseguire l'esportazione.

Esportazione delle pianificazioni in iCalendar

CA SDM consente di esportare Ordini di cambiamento nel formato iCalendar standard. Questo scambio di dati consente di importare le pianificazioni dell'Ordine di cambiamento in più applicazioni di gestione del calendario, inclusi Microsoft Outlook e Lotus Notes.

Nota: quando si esportano le pianificazioni in programmi per la gestione del calendario, la scelta dell'opzione Apri anziché Salva determina un'importazione non corretta del file. Per evitare questo problema nelle pianificazioni Gestione della conoscenza e Ordine di cambiamento, selezionare l'opzione Salva anziché Apri. Dopo avere salvato il file esportato, eseguirne l'importazione mediante l'interfaccia del programma del calendario. Non è possibile esportare le finestre del Cambiamento (blackout e manutenzione), ma solo gli Ordini di cambiamento.

Importante. I dati esportati sono basati sulla visualizzazione corrente. Se si desidera esportare un intervallo personalizzato di date, ad esempio 32 giorni, l'esportazione deve essere eseguita dalla visualizzazione di elenco. In caso contrario, la visualizzazione viene troncata ad un mese o una settimana. In questo modo viene esportata solo la quantità visibile.

Per visualizzare il calendario dei cambiamenti

1. Fare clic sulla scheda Calendario cambiamento.

   Vengono visualizzati i campi Filtro calendario cambiamento.

2. Completare i campi di ricerca per visualizzare una visualizzazione di calendario o elenco contenente gli Ordini di cambiamento desiderati.

3. Fare clic su Esporta.

   Viene visualizzata la pagina per l'esportazione delle pianificazioni.

   Importante. La variabile SchedExpMaximum in web.cfg controlla il numero massimo di eventi consentiti in un'esportazione. Incrementare il valore predefinito (1 000) può causare instabilità di sistema. Se si tenta di esportare un numero maggiore di eventi rispetto al valore specificato in SchedExpMaximum, viene visualizzato un messaggio che informa dell'impossibilità di eseguire l'esportazione.

4. Immettere la posizione in cui si desidera salvare un file iCalendar.

   Nella posizione specificata viene salvato un file iCalendar contenente tutti gli eventi della visualizzazione corrente.

Visualizzazioni di pianificazione

CA SDM fornisce le seguenti visualizzazioni di pianificazione:

Elenco

Visualizza una pagina elenco ordinata in base alla data di inizio e fine pianificazione.

Mese

Visualizza un calendario per un intero mese.

Questa visualizzazione mostra gli Ordini di cambiamento in gruppi. Ciascuna voce include uno o più Ordini di cambiamento. Per visualizzare le informazioni dettagliate relative agli Ordini di cambiamento di un gruppo posizionare il puntatore del mouse sul gruppo; premere ALT+FRECCIA DESTRA quando il gruppo è evidenziato oppure fare clic sul gruppo per mostrarne il contenuto in una visualizzazione n-giorni.

Settimana

Visualizza un'intera settimana in una sola colonna, partendo dal giorno configurato come primo della settimana.

Mostra le modifiche individualmente e include informazioni dettagliate su ogni Ordine di cambiamento pianificato durante la settimana.

Giorno

Visualizza gli Ordini di cambiamento relativi a un solo giorno.

Mostra le modifiche individualmente e include informazioni dettagliate su ogni Ordine di cambiamento pianificato durante il giorno.

***n* giorni**

Mostra gli Ordini di cambiamento per il numero di giorni specificati dal selettore a discesa.

Mostra le modifiche individualmente e include informazioni dettagliate su ogni Ordine di cambiamento pianificato durante i giorni selezionati.

Navigazione nelle visualizzazioni di pianificazione

È possibile utilizzare i tasti freccia e TAB per navigare nelle visualizzazioni di pianificazione. Sono disponibili i seguenti tasti di scelta rapida:

Tab

Passa a una data successiva. Premendolo quando si è nell'ultima cella si passa al pulsante Cerca.

Maiusc+Tab

Passa a una data precedente. Premendolo quando si è nella prima cella si passa al pulsante Mese successivo.

MAIUSC+freccia

Naviga nel calendario da data a data nella direzione della freccia.

Freccia destra

Visualizza il menu di scelta rapida per la data o l'evento attivi. In assenza di un menu di scelta rapida, passa alla data cronologicamente successiva (simile alla combinazione MAIUSC+freccia destra).

ALT+freccia destra

Visualizza un popup con informazioni a comparsa sulla data o sull'evento attivi. In assenza di informazioni a comparsa, passa alla data cronologicamente successiva (simile alla combinazione MAIUSC+freccia destra).

Freccia giù

Passa all'evento successivo nella cella corrente. Se la cella corrente non contiene eventi o se è già attivo l'ultimo evento, passa alla data nella successiva cella in basso (simile alla combinazione MAIUSC+freccia giù).

Freccia su

Passa all'evento precedente nella cella corrente. Se non è attivo un evento, passa alla data nella successiva cella in alto (simile alla combinazione MAIUSC+freccia su).

Tasti di scelta rapida per il calendario

Ogni visualizzazione di pianificazione supporta tasti di scelta rapida per i relativi pulsanti. Sono disponibili i seguenti tasti di scelta rapida:

MAIUSC+0

Passa alla visualizzazione elenco.

MAIUSC+1

Passa alla visualizzazione giornaliera.

MAIUSC+7

Passa alla visualizzazione settimanale.

MAIUSC+3

Passa alla visualizzazione mensile.

MAIUSC+9

Passa alla visualizzazione *n*-giorni.

MAIUSC+<

Passa al periodo di tempo precedente nella visualizzazione corrente.

MAIUSC+>

Passa al periodo di tempo successivo nella visualizzazione corrente.

Configurazione della visualizzazione di pianificazione

È possibile configurare le visualizzazioni di pianificazione mensili e settimanali specificando le istruzioni pdm_macro nella sezione <head> dei moduli HTMPL che definiscono la pianificazione. Si consiglia l'uso della visualizzazione Origine di Web Screen Painter per modificare questi moduli.

Qualsiasi modulo che visualizzi una pianificazione deve contenere quanto segue:

- Una macro schedConfig
- Almeno una macro schedAttr
- Almeno una macro schedGroup

Le macro di configurazione si trovano in un file fonte a parte, a cui l'istruzione pdm_include fa riferimento nel file fonte principale. Questo file consente di configurare la pianificazione senza modificare il file di origine principale.

Ad esempio, le macro di configurazione per il Modulo calendario cambiamento list_chgsched.htmpl si trovano in un file denominato list_chgsched_config.htmpl. Per la pianificazione relativa al ciclo di vita della conoscenza, è possibile modificare list_kdsched_config.htmpl utilizzando le stesse macro.

list_chgsched_config.htmpl e list_kdsched_config.htmpl si trovano nella seguente directory:

$NX_ROOT\bopcfg\www\htmpl\web\analyst\

Macro schedAttr — specificazione di un attributo archiviato

La macro schedAttr specifica un attributo archiviato per ogni elemento selezionato per l'elenco. Gli attributi archiviati sono disponibili per le informazioni a comparsa nella visualizzazione mensile, per le informazioni dettagliate o di riepilogo negli altri tipi di visualizzazione, e nella funzione JavaScript setSchedEvents(). I seguenti sono argomenti di macro validi:

attr=xxxx

(Obbligatorio) Specifica un attributo dall'oggetto nella pianificazione, come un ordine di cambiamento o un documento della conoscenza. Gli attributi puntati sono ammessi. Nel calendario dei cambiamenti è possibile utilizzare il nome attributo di parola chiave CI*nn* per specificare che i primi elementi della configurazione *nn* associati all'ordine di cambiamento sono inclusi nelle informazioni memorizzate.

Nota: questo è l'unico argomento richiesto per la macro schedAttr.

attrRef=.COMMON_NAME|xxxx

Memorizza l'attributo della tabella di riferimento memorizzata per un attributo SREL (ignorato per gli attributi non-SREL). Il nome dell'attributo specificato deve essere preceduto da un punto.

Impostazione predefinita: .COMMON_NAME

label=

Visualizza un'etichetta per l'attributo nella visualizzazione n-giorni.

Impostazione predefinita: il DISPLAY_NAME Majic dell'attributo

ident=1|0

Specifica se l'attributo è un identificatore per l'oggetto (come un numero di riferimento di un ordine di cambiamento). Gli attributi identificatore vengono visualizzati senza etichetta di fronte al nome del gruppo nelle informazioni a comparsa e nella visualizzazione n-giorni.

Impostazione predefinita: 0

detail=1|0

Specifica se l'attributo è incluso nelle informazioni dettagliate contenute in visualizzazioni diverse da quella mensile. Le informazioni dettagliate sono comprese nelle informazioni visualizzate quando la casella di controllo per la visualizzazione del solo riepilogo non è selezionata.

Impostazione predefinita: 1

hoverInfo=1|0

Specifica se l'attributo è incluso nel popup delle informazioni a comparsa visualizzate nella visualizzazione mensile passando con il mouse su un gruppo o premendo MAIUSC+freccia destra quando il gruppo è selezionato.

Impostazione predefinita: 0

summary=1|0

Specifica se l'attributo è incluso nelle informazioni dettagliate contenute in visualizzazioni diverse da quella mensile. Le informazioni dettagliate sono comprese nelle informazioni visualizzate quando la casella di controllo per la visualizzazione del solo riepilogo non è selezionata.

Impostazione predefinita: 0

Nota: CA SDM visualizza gli attributi in informazioni di riepilogo, dettagliate o a comparsa nello stesso ordine delle rispettive macro schedAttr.

Macro schedConfig — programmazione della configurazione

La macro schedConfig specifica che un modulo contiene una pianificazione e fornisce informazioni di configurazione base. I seguenti sono argomenti di macro validi:

autosearch=1|0

Specifica se il modulo di pianificazione ricarica i dati dal server quando l'utente seleziona una visualizzazione al di fuori dell'intervallo date attualmente selezionato. Se si imposta il valore su 1 (valore predefinito), il modulo esegue automaticamente la ricerca quando l'utente seleziona una visualizzazione con uno o più giorni non compresi nell'intervallo di selezione date del filtro di ricerca. Se si imposta il valore su 0, l'utente deve premere il pulsante Cerca per avviare una ricerca.

defaultView=0|1|7|30|99

Specifica la visualizzazione predefinita per il filtro di ricerca come 0 (elenco), 1 (giorno), 7 (settimana), 30 (mese) o 99 (n-giorni).

La specificazione per defaultView interessa solo la visualizzazione iniziale del filtro di ricerca. Una volta visualizzata la pianificazione, CA SDM mantiene automaticamente la selezione di visualizzazione filtro allineata con la visualizzazione corrente.

Impostazione predefinita: 30

firstday=0|1|2|3|4|5|6|7

Specifica il primo giorno della settimana nella visualizzazione mensile come numero compreso tra 0 (domenica) e 6 (sabato).

Impostazione predefinita: 0

export=xxx|0

Specifica il nome di codice del modello utilizzato per l'esportazione nel formato iCalendar. Se si imposta il valore su 0, la funzionalità e il pulsante di esportazione saranno disattivati.

Impostazione predefinita: ChangeSchedule

legend=1|2|0

Specifica la posizione della legenda di pianificazione che mostra il nome e la formattazione dei gruppi nella pianificazione. Impostare il valore su 1 per posizionare la legenda sopra la panificazione, 2 per posizionarla sotto la pianificazione. Impostare il valore su 0 per disattivare la legenda.

Impostazione predefinita: 2

maxGroups=0/*n*

Specifica il numero massimo di gruppi da visualizzare in una sola cella della visualizzazione mensile del calendario.

Se i gruppi pianificati per un solo giorno superano il valore maxGroups, CA SDM visualizza soltanto i primi maxGroups-1, e sostituisce gli ultimi con un collegamento ipertestuale "..altri nn cambiamenti", che consente di visualizzare l'intero elenco al passaggio del mouse o facendo clic. Impostare il valore su 0 per disattivare questa funzionalità e consentire un numero illimitato di eventi in una cella di calendario.

Impostazione predefinita: 4

nday=(n,n,...)

Specifica le selezioni per l'elenco a discesa della visualizzazione n-giorni.

La specificazione è un elenco di conteggi di giorni da includere nell'elenco a discesa, oppure uno 0 per indicare che l'elenco a discesa n-giorni è escluso dalla pianificazione. Il primo valore specificato è l'impostazione predefinita per l'elenco a discesa.

Impostazione predefinita: (3,7,14,28)

round=(*h*,*min*)|0

Specifica se le date di inizio e di fine pianificazione vengono arrotondate quando si raccolgono ordini di cambiamento o strumenti della conoscenza in gruppi. Specificare round=0 per disattivare l'arrotondamento.

Per impostazione predefinita, oggetti dei gruppi data di inizio e fine pianificazione. Tutte le date di CA SDM includono l'ora e, senza l'arrotondamento, gli oggetti pianificati con anche un solo minuto di differenza si troveranno in gruppi distinti. L'arrotondamento determina il gruppo dopo la modifica dell'ora di inizio a un'ora o un minuto precedenti l'ora di fine a un'ora o un minuto successivi.

Il valore di arrotondamento specifica un'ora o un minuto (ma non entrambi). Le ore vengono arrotondate al multiplo più vicino del valore specificato, ad esempio:

round=(0,15) arrotonda al quarto d'ora più vicino

round=(30) arrotonda alla mezzora più vicina

round=1	arrotonda all'ora più vicina
round=12	arrotonda alla mezza giornata più vicina (00:00 o 12:00)
round=24	arrotonda al giorno più vicino

Impostazione predefinita: (0,15)

timefmt=24hr|([am],[pm])

Specifica il formato degli orari nelle visualizzazioni del calendario della pianificazione.

Il valore predefinito di 24 ore specifica che gli orari vengono visualizzati nel formato a 24 ore (0:01 - 23:59). Il valore alternativo (am,pm) specifica un suffisso per le ore antimeridiane o pomeridiane, oppure per entrambe.

Nota: tutti gli argomenti schedConfig sono opzionali.

Macro schedGroup — specificazione di un gruppo eventi

La macro schedGroup specifica il nome e il codice colore di un gruppo di elementi. La visualizzazione mensile aggrega tutti gli elementi di un gruppo in un unico evento. Tutte le visualizzazioni eccetto quella mensile mostrano gli elementi individuali nel formato per il gruppo a cui appartengono. I seguenti sono argomenti di macro opzionali:

grpname=xxx

(Obbligatorio) Specifica il nome del gruppo. La macro assegna automaticamente un numero al gruppo e lo assegna a una variabile JavaScript con un nome del modulo schedGroup_xxx, in cui xxx è il nome del gruppo. Questa variabile può essere utilizzata nella funzione JavaScript setSchedEvents() per creare un evento appartenente al gruppo.

Nota: questo è l'unico argomento richiesto per la macro schedGroup.

label=xxx

Specifica un'etichetta per il gruppo. Se specificato, l'etichetta compare in tutte le visualizzazioni.

legend=xxx|0

Visualizza una descrizione del gruppo per la legenda che compare in fondo alla pianificazione. I gruppi compaiono nella legenda se ne esiste almeno un esempio nella visualizzazione corrente. Se si specifica 0 il gruppo sarà sempre escluso dalla legenda.

Impostazione predefinita: 0

color=black|*color*

Specifica il colore del testo negli elementi del gruppo in questione. I colori possono essere specificati in formato CSS; o un colore Web valido o un valore decimale preceduto dal segno del cancelletto.

Esempio: per il rosso immettere "#FF0000" o "red".

Impostazione predefinita: nero

bgcolor=white|*color*

Specifica il colore dello sfondo negli elementi del gruppo in questione. I colori dello sfondo possono essere specificati in formato CSS; o un colore Web valido o un valore decimale preceduto dal segno del cancelletto.

Esempio: per il rosso immettere "#FF000" o "red".

Impostazione predefinita: bianco.

style=normal|bold|italic

Specifica lo stile del testo per il gruppo negli stili normale, grassetto o corsivo.

Impostazione predefinita: normale

Configurazione delle finestre di blackout e di manutenzione nel calendario dei cambiamenti

Per cambiare colori, etichette, legende e icone delle finestre di cambiamento, è necessario modificare le istruzioni PDM_MACRO del file list_chgsched_config.htmpl .

Nota: se si utilizzano le macro schedGroup per modificare la formattazione delle finestre nel calendario dei cambiamenti, è inoltre necessario aggiornare il file *schedule.css* per fare in modo che la formattazione sia conforme a quella dell'utilità di pianificazione dei cambiamenti.

Per configurare finestre di cambiamento

1. Aprire il modulo *list_chgsched_config.htmpl* in un editor di testo o in Web Screen Painter.

   Questo file si trova nella directory seguente:

   ```
   $NX_ROOT\bopcfg\www\htmpl\web\analyst\
   ```

2. Nella macro schedGroup, modificare le seguenti istruzioni PDM_MACRO:

   Per le finestre di manutenzione:

   ```
   <PDM_MACRO NAME=schedGroup grpname=maintWindow
       bgcolor=lightgreen
       label="Maintenance"
       legend="Maintenance Window"
       icon= "confirmation_12.png">
   ```

   Per le finestre di blackout:

   ```
   <PDM_MACRO NAME=schedGroup grpname=blackoutWindow style=italic color=white
       bgcolor=black
       label="Blackout"
       legend="Blackout Window"
       icon= "warning_12.png">
   ```

   bgcolor

   Specifica il colore dello sfondo della finestra.

   etichetta

   Specifica l'etichetta della finestra come Blackout o Manutenzione.

   legend

   Specifica il testo della legenda così come viene visualizzata nel calendario dei cambiamenti.

   icon

   Specifica un URL opzionale a un oggetto grafico Web di 12x12 pixel.

Questa icona viene visualizzata insieme a un Ordine di cambiamento o a un gruppo nel calendario dei cambiamenti se l'Ordine di cambiamento rientra completamente in una finestra di manutenzione o si sovrappone a una finestra di blackout.

3. Salvare il modulo.

   La finestra Cambiamento viene configurata.

La funzione JavaScript setSchedEvents()

La funzione JavaScript setSchedEvents() crea eventi nella pianificazione. Modificare questa funzione per visualizzare nuovi oggetti di gruppo. Gli oggetti di gruppo predefiniti vengono visualizzati per impostazione predefinita.

CA SDM richiama setSchedEvents() una volta per ciascun oggetto (Ordine di cambiamento o documento della conoscenza) selezionato dal filtro di ricerca di pianificazione. La funzione crea eventi per l'oggetto richiamando una seconda funzione, schedEvent(), e trasferendo l'ID di gruppo, la data d'inizio e la data di fine dell'evento.

La funzione può creare un numero illimitato di eventi (compreso zero) per un oggetto. La funzione setSchedEvents() predefinita per il calendario dei Cambiamenti (list_chgsched.htmpl) crea un evento per ogni Ordine di cambiamento e li raggruppa in base al tipo di Cambiamento. Questa funzione è codificata come segue:

```
1.      function setSchedEvents( chg )
2.      {
3.      var grpnum;
4.      switch( chg["chgtype"] - 0 ) {
5.              case 100: grpnum = schedGroup_std;  break;
6.              case 300: grpnum = schedGroup_std;  break;
7.              default:  grpnum = schedGroup_norm; break;
8.      }
9.      chg.schedEvent( grpnum, chg["sched_start_date"], chg["sched_end_date"] );
10.     }
```

Il parametro case specifica l'ID del tipo di cambiamento. Per elencare gli ID caso, consultare Creazione di un tipo di modifica.

La funzione ha un solo argomento di un oggetto JavaScript contenente gli attributi specificati dalle macro schedAttr. L'istruzione switch nelle righe 4-8 esamina l'attributo chgtype dell'Ordine di cambiamento e assegna il numero di gruppo appropriato da una delle variabili schedGroup_xxxx definite da precedenti macro schedGroup. Alla riga 9, richiama la funzione schedEvent() per creare un evento nella pianificazione, passando il numero di gruppo precedentemente assegnato e le date di inizio e fine pianificazione. Le date sono disponibili nell'oggetto argomento perché sono state specificate in precedenti macro schedAttr.

Modalità di pianificazione degli Ordini di cambiamento

È possibile visualizzare la pianificazione di tutti gli elementi della configurazione associati a un Ordine di cambiamento Quando si crea, modifica o visualizza un Ordine di cambiamento o si aggiorna il calendario dei Cambiamenti è utile controllare le informazioni di pianificazione. La visualizzazione della pianificazione è utile per evitare possibili conflitti.

Per visualizzare e aggiornare una pianificazione, effettuare le seguenti operazioni:

1. Creare o aprire un Ordine di cambiamento.
2. Associare gli elementi della configurazione all'Ordine di cambiamento.

   Nota: se non associa un elemento della configurazione all'Ordine di cambiamento, si verificherà un errore quando si fa clic sul pulsante Utilità di pianificazione.
3. Fare clic su Visualizza utilità di pianificazione.

   Viene visualizzata l'utilità di pianificazione dei cambiamenti, che include le seguenti visualizzazioni:

   Quotidiano

   (Predefinito) Visualizza il periodo dell'Ordine di cambiamento per la data e l'ora selezionate. Se non è associata alcuna data all'Ordine di cambiamento, la visualizzazione predefinita è impostata sul giorno corrente.

   Settimanale

   Visualizza il periodo dell'Ordine di cambiamento nella settimana corrente e include la data di inizio implementazione, che può essere impostata sulla data di inizio del calendario dei Cambiamenti.

   Nota: la durata della pianificazione determina la lunghezza di ombreggiatura nella pianificazione. Ad esempio, se si crea un Ordine di cambiamento con una durata di due ore, l'ombreggiatura in giallo chiaro nell'utilità di pianificazione corrisponde alle due ore della durata definita.
4. (Facoltativo) Fare clic su un elemento della configurazione per visualizzarne i dettagli. Passare con il puntatore sul nome dell'elemento della configurazione per visualizzarne il nome completo.
5. (Facoltativo) Modificare la data di inizio dell'implementazione o la durata.
   a. Fare clic su Visualizza pianificazione per vedere in anteprima la pianificazione aggiornata.
   b. Fare clic su Aggiorna pianificazione per aggiornare la pianificazione.

   Nota: è possibile cambiare la pianificazione solo in modalità di modifica.
6. Salvare l'Ordine di cambiamento.
7. Aggiornare il calendario dei cambiamenti per visualizzare finestre di Cambiamento globali e associate a elementi della configurazione.

Esempio di utilizzo dell'utilità di pianificazione dei cambiamenti

L'esempio seguente dimostra come utilizzare l'utilità di pianificazione dei cambiamenti quando si crea un ordine di cambiamento.

1. Selezionare File, Nuovo ordine di cambiamento nella scheda Service Desk.

   Viene visualizzata la pagina Crea nuovo ordine di cambiamento.

2. Selezionare Aggiorna elementi della configurazione nella scheda Elementi di configurazione.

   Viene visualizzata la pagina Ricerca elemento della configurazione.

3. Creare o cercare elementi della configurazione.

4. Utilizzando la pagina Aggiorna elementi della configurazione interessati, aggiungere elementi della configurazione all'ordine di cambiamento.

5. Fare clic su OK.

   La pagina Crea nuovo ordine di cambiamento viene aggiornata.

6. Fare clic sul pulsante Utilità di pianificazione.

   Viene visualizzata la pagina Pianificazione ordini di cambiamento.

7. Selezionare una vista ed effettuare *una qualsiasi* delle operazioni seguenti:

   - Fare clic nelle celle della tabella per modificare la data di inizio pianificazione.
   - Fare clic su Data inizio pianificazione per utilizzare l'assistente delle date.

8. Modificare la durata e fare clic su Visualizza pianificazione.

   Nella pianificazione viene visualizzata un'anteprima dei cambiamenti.

9. Fare clic su Aggiorna pianificazione.

   La pianificazione viene aggiornata con i cambiamenti.

10. Salvare l'ordine di cambiamento.

Impostazione del numero massimo di elementi della configurazione

È possibile impostare il numero massimo di elementi della configurazione che compaiono nell'utilità di pianificazione dei cambiamenti.

Per impostare il numero massimo di elementi della configurazione

1. Aprire il file *NX.env*.

   Questo file si trova nella directory seguente:

   ```
   $NX_ROOT\
   ```

2. Modificare il valore di *@NX_CHANGE_SCHEDULER_MAX_CI_CNT* specificando il numero massimo desiderato.

   Nota: per impostazione predefinita, la variabile è impostata su 100. Se il numero massimo di elementi della configurazione è impostato su un valore maggiore di 100, vengono visualizzati solo i primi 100 elementi e compare un avviso.

3. Salvare il file *NX.env* e riavviare CA SDM.

   Il numero massimo di elementi della configurazione viene impostato.

Esempio: impostazione del numero massimo di elementi della configurazione su 25

Con l'impostazione seguente, nell'utilità di pianificazione dei cambiamenti vengono visualizzati solo i primi 25 elementi della configurazione.

```
@NX_CHANGE_SCHEDULER_MAX_CI_CNT=25
```

Modifica del colore dello sfondo per la durata di un ordine di cambiamento

È possibile modificare il colore dello sfondo per la durata di un ordine di cambiamento. Modificare le righe seguenti nel file *schedule.css* per modificare l'evidenziare della barra verde per la durata di un ordine di cambiamento.

Per modificare il colore dello sfondo

1. Aprire il file *schedule.css*.

   Questo file si trova nella directory seguente:

   `$NX_ROOT\bopcfg\www\wwwroot\css`

   Importante anche la directory $NX_ROOT\sdk contiene un file chiamato schedule.css, che contiene informazioni utili sui controlli CSS.

2. Modificare le righe seguenti specificando il codice di colore desiderato:

   ```
   td.noBorderBackColor{border-left:none;border-right:none;background-color:#F6E
   3CE;}
   td.withBorderBackColor{border-right:none;border-left:1px
   solid;background-color:#F6E3CE;}
   ```

3. Salvare il file *schedule.css*.

Nell'esempio seguente, il colore dello sfondo per la durata del cambiamento è #FF0000.

Esempio: modifica del colore dello sfondo per la durata del cambiamento in #FF0000

```
td.noBorderBackColor{border-left:none;border-right:none;background-color:#FF0000;
}
td.withBorderBackColor{border-right:none;border-left:1px
solid;background-color:#FF0000;}
```

Modifica dei colori delle finestre di cambiamento nell'utilità di pianificazione dei cambiamenti

È possibile cambiare i colori che indicano le finestre di cambiamento modificando righe del file *schedule.css.*

Nota: se si modifica il file *schedule.css* per cambiare la formattazione delle finestre nell'utilità di pianificazione dei cambiamenti, è inoltre necessario modificare le macro schedGroup utilizzate dal calendario dei cambiamenti per fare in modo che la formattazione sia conforme a quella dell'utilità di pianificazione.

Per modificare il colore dello sfondo

1. Aprire il file *schedule.css* in un editor di testo.

   Questo file si trova nella directory seguente:

   ```
   $NX_ROOT\bopcfg\www\wwwroot\css
   ```

2. Modificare le righe seguenti specificando il codice di colore desiderato:

   ```
   .schedConflict { background-color: #ff0000; font-size: 4px }
   .schedBusy { background-color: #0176ff; font-size: 4px}
   .schedCurrent { background-color: #008000; font-size: 4px; }
   .schedMW { background-color: #40ff40; font-size: 4px; }
   .schedBW { background-color: black; font-size: 4px; }
   .schedNone {font-size: 4px; }
   .schedDialog { width: 100%; height: 4px; margin-left: 0px; margin-right: 0px;
   margin-top: 4px; margin-bottom: 4px; }
   ```

3. Salvare il file *schedule.css*.

   Il colore dello sfondo viene modificato.

Ulteriori informazioni:

Macro schedConfig — programmazione della configurazione (a pagina 805)

Modalità di pianificazione delle finestre di cambiamento

È possibile pianificare le finestre di cambiamento e visualizzarle nel calendario dei cambiamenti. Le *finestre di manutenzione* stabiliscono i periodi di tempo in cui dovrebbero avvenire i cambiamenti degli elementi della configurazione, mentre le *finestre di blackout* stabiliscono i peridi in cui *non* dovrebbero avvenire i cambiamenti degli elementi della configurazione. Le finestre di cambiamento consentono di pianificare i cambiamenti in modo da ridurne al minimo l'impatto sui processi di business critici. CA SDM può implementare le finestre di cambiamento a livello globale o di sistema.

Per pianificare le finestre di cambiamento, procedere come segue:

1. Visualizzare il calendario dei cambiamenti per vedere dove si desiderano delle finestre di cambiamento.
2. Creare le finestre di cambiamento appropriate per la propria organizzazione.

   Finestra di manutenzione

   Indica un periodo pianificato durante il quale è possibile cambiare uno o più elementi della configurazione. Dato che i cambiamenti possono comportare tempi di inattività, si possono utilizzare queste finestre per ridurre al minimo l'interruzione dei processi di business. In generale, i cambiamenti pianificati devono avere luogo in una finestra di manutenzione.

   Finestra di blackout

   Indica un periodo pianificato durante il quale non devono essere effettuati cambiamenti agli elementi della configurazione. Questa finestra di blackout può indicare un periodo di supporto ridotto (ad esempio, una vacanza), un evento aziendale o un periodo lavorativo critico, come la fine dell'anno fiscale. In generale, i cambiamenti pianificati devono avere luogo solo al di fuori delle finestre di blackout.

   Finestra Cambiamento globale

   Indica una finestra di manutenzione o blackout che interessa l'intera organizzazione. Ad esempio, si desidera creare una finestra di blackout globale (a pagina 820) denominata Vacanze che abbia inizio a novembre e termini a gennaio, con fuso orario Est americano. Questa finestra di interruzione *non* consente Cambiamenti non di emergenza nell'intervallo compreso tra le date specificate. Le finestre di Cambiamento globale non vengono associate a elementi della configurazione specifici perché vengono applicate a tutti gli elementi della configurazione.

3. (Facoltativo) Specificare i criteri di ricorrenza delle finestre di cambiamento.
4. Aprire il calendario dei cambiamenti.

   La legenda mostra icone e colori che identificano le finestre di cambiamento nella pianificazione.

5. Creare gli Ordini di cambiamento associati agli elementi della configurazione.

6. Aprire il calendario dei Cambiamenti mediante l'utilità di pianificazione del Cambiamento.

Nota: per ulteriori informazioni sulla creazione delle finestre di Cambiamento, consultare la *Guida in linea*.

Visualizzazione di finestre di cambiamento

È possibile visualizzare finestre di cambiamento nel calendario dei cambiamenti per vedere se è possibile modificare o meno elementi della configurazione associati.

Per visualizzare finestre di cambiamento

1. Nella scheda Amministrazione, fare clic su Service Desk, Ordini di cambiamento, Finestre di cambiamento.

   Viene visualizzato l'Elenco finestre di cambiamento.

2. Selezionare la finestra di cambiamento che si desidera visualizzare.

   Viene visualizzata la finestra di cambiamento.

3. (Facoltativo) Fare clic su Modifica.

   È possibile modificare la finestra di cambiamento.

4. Salvare o chiudere la finestra.

   Viene visualizzata la pagina Dettagli finestra.

Associazione di un elemento della configurazione con una finestra di manutenzione

Per controllare quando un elemento della configurazione viene sottoposto a manutenzione, è possibile associarlo a una finestra di manutenzione.

Per associare un elemento della configurazione con una finestra di manutenzione

1. Accedere alla pagina Dettagli finestra di cambiamento.
2. Fare clic sulla scheda Elementi della configurazione associati.

   Viene visualizzato l'elenco degli elementi della configurazione associati.
3. Fare clic su Aggiorna elementi della configurazione.

   Viene visualizzata la pagina Ricerca elemento della configurazione.
4. Specificare i dati dell'elemento della configurazione desiderato.
5. Fare clic su Cerca

   Viene visualizzata la pagina Elementi della configurazione disponibili.
6. Spostare gli elementi della configurazione desiderato dall'elenco degli elementi della configurazione disponibili a quello degli elementi associati.
7. Fare clic su OK.

   Viene visualizzata la pagina Dettagli finestra di cambiamento.
8. Fare clic su Salva.

   L'elemento della configurazione è associato a una finestra di manutenzione.

La finestra di cambiamento, gli elementi della configurazione e le associazioni di finestra selezionati vengono salvati.

Visualizzazione di elementi della configurazione associati

Per stabilire quali elementi della configurazione potrebbero venire influenzati in determinati periodi di tempo, è possibile visualizzare gli elementi della configurazione che sono associati a finestre di manutenzione non globali.

Per visualizzare elementi della configurazione associati a una finestra di manutenzione

1. Accedere alla pagina Dettagli finestra di cambiamento.
2. Fare clic sulla scheda Elementi della configurazione associati.

   Vengono visualizzati gli elementi della configurazione associati.

Esempio di creazione di una finestra di blackout

L'esempio seguente crea una finestra di blackout indicante che l'organizzazione non deve pianificare gli Ordini di cambiamento per un periodo di tempo specifico. Questa finestra di blackout dura 48 ore e si ripete ogni venerdì alle 18.00 del proprio fuso orario.

Procedere come descritto di seguito:

1. Nella scheda Amministrazione, fare clic su Service Desk, Ordini di cambiamento, Finestre di cambiamento.

   Viene visualizzato l'Elenco finestre di cambiamento.

2. Fare clic su Crea nuovo.

   Viene visualizzata la pagina Crea nuova finestra di cambiamento.

3. Completare i campi nel modo seguente:

   a. Immettere **Friday_Blackout** come nome della finestra.

   b. Selezionare il tipo Blackout.

   c. Selezionare lo stato Attivo.

   d. Selezionare come data di inizio il prossimo venerdì e le ore 18.00 dall'assistente delle date.

   e. Selezionare come data di fine la prossima domenica e le ore 18.00 dall'assistente delle date.

   f. Selezionare il proprio fuso orario.

   g. (Facoltativo) Immettere una descrizione per la finestra di blackout.

   h. Nella scheda Schema di ricorrenza, selezionare Settimanale.

      - Impostare la ricorrenza su ogni settimana (**1**).
      - Selezionare la data di fine della ricorrenza.

4. Salvare e chiudere la finestra di blackout.

5. Aggiornare l'elenco Elenco finestre di cambiamento.

6. Aprire e aggiornare il calendario dei cambiamenti.

   La finestra di blackout compare nella pianificazione.

Creazione di una finestra di manutenzione globale

Creare una finestra di manutenzione globale per la propria organizzazione. Ad esempio, *non* si desidera definire le finestre di manutenzione per il server o l'elemento della configurazione e si desidera completare i Cambiamenti globali durante i weekend.

Procedere come descritto di seguito:

1. Accedere alla pagina Elenco finestre di cambiamento.
2. Fare clic su Crea nuovo.
3. Viene visualizzata la pagina Crea nuova finestra di cambiamento.
4. Immettere o modificare i campi desiderati per creare la finestra di manutenzione.
5. Impostare il campo Tipo su Manutenzione.
6. Verificare che la casella di controllo Globale sia selezionata.

   Nota: una finestra di manutenzione globale non può essere associata a elementi della configurazione.
7. Immettere la data di inizio, la data di fine e il fuso orario.
8. Fare clic su Salva.

   La finestra di manutenzione globale viene salvata.

Analisi e rilevamento dei conflitti

L'analisi dei conflitti rileva e visualizza le discrepanze che si presentano quando due o più cambiamenti dello stesso elemento della configurazione sono pianificati per essere implementati alla stessa ora. Il gruppo di gestione dei cambiamenti si occupa di risolvere i conflitti di pianificazione come segue:

- Utilizza il calendario dei cambiamenti per visualizzare gli eventuali conflitti di elementi della configurazione provocati da Ordini di cambiamento e apporta le modifiche necessarie per ridurne l'impatto.
- Cerca e rileva i conflitti in un registro.

Nota: per ulteriori informazioni sulla gestione dei conflitti di pianificazione, vedere la *Guida in linea*.

Visualizzazione di CA Workflow

La visualizzazione di CA Workflow consente di controllare l'avanzamento delle attività di flusso di lavoro per un ordine di cambiamento. Il visualizzatore dei processi mostra graficamente ogni passaggio del processo CA Workflow, compresi quelli completati o incompleti e lo stato corrente dell'avanzamento del flusso di lavoro.

Il visualizzatore dei processi mostra lo stato e il percorso di un processo CA Workflow Elaborare quando è associato a una categoria di cambiamento/questione o a un'area di richiesta/incidente/problema.

Modalità di visualizzazione del flusso di lavoro

Visualizzare il flusso di lavoro come descritto di seguito:

1. Associare un processo CA Workflow ad una categoria Cambiamento.
2. Creare un Ordine di cambiamento utilizzando questa categoria di Cambiamento.
3. Nella scheda Attività flusso di lavoro, fare clic sul pulsante Visualizza processo per avviare il visualizzatore dei processi.

Nota: per ulteriori informazioni su come associare i processi CA Workflow a categorie o aree, vedere la *Guida in linea*.

Esempio di utilizzo del visualizzatore dei processi

Questo esempio dimostra come utilizzare il visualizzatore dei processi sul sistema utilizzando una categoria di cambiamento predefinita, dopo aver installato CA Workflow e aver attivato le opzioni.

1. Nella scheda Amministrazione accedere a Service Desk, Ordini di cambiamento, Categorie.

   Viene visualizzata la pagina Elenco Categorie Cambiamento.

2. Selezionare Add.IT.Other dalla colonna Simbolo.

   Viene visualizzata la pagina Dettagli categoria Cambiamento Add.IT.Other.

3. Fare clic su Modifica.

   Viene visualizzata la pagina Aggiorna categoria Cambiamento Add.IT.Other.

4. Fare clic sulla scheda Flusso di lavoro.

   Fare clic sulla casella di controllo CA Workflow.

   Viene visualizzato l'Elenco definizioni flusso di lavoro.

5. Selezionare Ordine PC - Service Desk Versione 12.9.

   Il nome del processo viene inserito nel campo Nome definizione CA Workflow.

6. Fare clic su Salva.

   Viene visualizzata la pagina Dettagli categoria Cambiamento.

7. Chiudere la finestra.

8. Creare e salvare un Ordine di cambiamento utilizzando la categoria Add.IT.Other.

   La scheda Attività flusso di lavoro mostra il processo Ordine PC - Service Desk Versione 12.9 e l'elenco degli elementi di lavoro.

9. Fare clic sul pulsante Visualizza processo nella scheda Attività flusso di lavoro.

   Viene visualizzato Process Viewer.

   Nota: è possibile visualizzare il progresso aggiornato delle attività flusso di lavoro aggiornando il visualizzatore dei processi.

Definizione del processo Gestione Cambiamento per CA Workflow

La definizione del processo di gestione dei Cambiamenti gestisce gli Ordini di cambiamento Standard, Normale o Emergenza. In quanto parte di CA Workflow, la definizione del processo di gestione dei Cambiamenti gestisce tutte le attività relative agli Ordini di cambiamento dalla richiesta iniziale di Cambiamento fino all'esame post-implementazione. Man mano che ciascuna attività viene completata, la definizione del processo Gestione Cambiamento aggiorna lo stato dell'Ordine di cambiamento e il registro delle attività. La definizione del processo Gestione Cambiamento invia anche al contatto o gruppo un messaggio di posta elettronica contenente le attività che devono essere completate.

La definizione del processo Gestione Cambiamento include le seguenti funzionalità:

- Analizza il tipo di Ordine di cambiamento e il livello di rischio associato per determinare il livello di approvazioni necessario per l'implementazione del Cambiamento.
- Fornisce una base di esempio da usare come riferimento per la gestione dei Cambiamenti.
- Si allinea con gli standard ITIL v3 per la valutazione dei rischi, l'analisi dell'impatto e conflitti, e le approvazioni effettuate da Gestione Cambiamento e CAB.
- Integra le seguenti funzionalità di Gestione Cambiamento CA SDM:
    - Indagine di valutazione rischio
    - Caso di business
    - Analisi dei conflitti
    - Analisi dell'impatto
    - Codici di chiusura
    - Codici di stato
    - Tipo di cambiamento
    - Flag di approvazione CAB e CAB

Ulteriori informazioni:

CA Workflow (a pagina 389)

Componenti della definizione di processo della Gestione cambiamento

La definizione di processo della Gestione cambiamento ha i seguenti componenti:

- **Definizione di processo della Gestione cambiamento**—La definizione di processo che gestisce l'intero processo di ordine di cambiamento. Tutte le attività e sottoattività seguono le attuali migliori pratiche di CA Workflow per la gestione delle eccezioni. Il nome del file della definizione di processo è *r12_Change_Mgmt_[en_lingua].xml*. Per esempio, il nome della definizione di processo in inglese è r12_Change_Mgmt_en_US.xml.

  Nota: per informazioni riguardo alle migliori pratiche di CA Workflow, consultare https://support.ca.com/irj/portal/anonymous/phpdocs?filePath=0/7956/7956_tecdoc.html.

- **Ottenere membri del gruppo e definizione di processo di notifica**—Un blocco di costruzione che gestisce le notifiche via e-mail per gruppi. La definizione del processo di acquisizione della memoria e notifica accetta l'UUID del gruppo come input. A seconda del flag di notifica, la definizione del processo di acquisizione della memoria e notifica può inviare un messaggio di posta elettronica a ciascun membro del gruppo oppure solo al manager del gruppo. Il nome del file della definizione del processo è *r12_Get_Group_Mem_Notify_[en_language].xml.* Ad esempio, il nome del file della definizione del processo è r12_Change_Mgmt_en_US.xml.

- **Acquisizione memoria gruppo e notifica attore**—Un attore che chiama la definizione del processo di acquisizione della memoria e notifica. Il nome del file dell'attore è *r12_Get_Group_Mem_Notify_Actor_[en_language].xml*. Ad esempio, il nome del file dell'attore inglese è r12_Get_Group_Mem_Notify_Actor_en_US.xml.

- **Conversione data e ora**—Un attore che accetta la data e l'ora come input e fornisce una stringa data e ora leggibile per i campi Data di inizio prevista e Data di fine prevista nei moduli di approvazione. L'attore di conversione della data e l'ora è un attore JavaScript CA Workflow. Il nome del file dell'attore è *r12_Date_Time_Convert_Actor_[en_language].xml*. Ad esempio il nome del file dell'attore inglese è r12_Date_Time_Convert_Actor_en_US.xml.

Come configurare la definizione dei processi di gestione dei cambiamenti

Per configurare la definizione dei processi di gestione dei cambiamenti, effettuare le seguenti operazioni:

1. Utilizzare CA Workflow per esaminare la documentazione (a pagina 825) relativa ai nodi di attività, alle attività secondarie e alle notifiche.

2. Creare i gruppi di implementazione e CAB (a pagina 827) responsabili della gestione del processo di cambiamento.

3. Creare contatti (a pagina 828) e assegnarli ai gruppi di implementazione o CAB.
4. Configurare le notifiche di posta elettronica (a pagina 826) per la definizione dei processi di gestione dei cambiamenti.
5. Se non si utilizza la porta del server Tomcat predefinita 8090, configurare il server Tomcat (a pagina 829) per le comunicazioni appropriate tra CA Workflow e CA SDM.
6. Configurare una o più categorie di cambiamento (a pagina 829) per utilizzare la definizione dei processi di gestione dei cambiamenti.
7. Installare l'opzione Impostazioni predefinite categoria (a pagina 830) in Gestione opzioni.

Visualizzare la documentazione circa nodi di attività e attributi

Dato che tutti i nodi di attività e gli attributi all'interno della Definizione processo Gestione cambiamento sono documentati, è possibile utilizzare CA Workflow per visualizzare informazioni riguardo ai nodi di attività e agli attributi. Se necessario, è possibile modificare il flusso della definizione di processo per andare incontro alle esigenze della propria organizzazione.

Nota: per informazioni riguardo alla visualizzazione di nodi di attività e attributi, consultare la documentazione di CA Workflow.

Per visualizzare la documentazione circa nodi di attività e attributi

1. Aprire la definizione di processo di Change Mgmt – Service Desk r12.1 nell'applicazione CA Workflow.

   Compare in CA Workflow la Definizione processo Gestione cambiamento.
2. Fare doppio clic su un nodo attività.

   Si apre il nodo attività.
3. Nella scheda Proprietà, consultare il campo Descrizione per ulteriori dettagli riguardo al nodo.
4. Uscire dalle proprietà del nodo attività.
5. (Facoltativo) selezionare la scheda Attributi nella finestra inferiore della definizione di processo.
6. Fare doppio clic o spostare il puntatore del mouse sull'attributo.

   Si apre la pagina Attributo con informazioni riguardo all'attributo.

Visualizzazione delle sotto-attività

La definizione del processo Gestione Cambiamento utilizza numerose sotto-attività CA Workflow per semplificare il flusso di lavoro. Quando si utilizza la definizione del processo Gestione Cambiamento, è possibile rivedere ed eventualmente personalizzare le sotto-attività.

Per visualizzare le sotto-attività:

1. Aprire la definizione del processo Gestione Cambiamento – Service Desk r12,1 nell'applicazione CA Workflow.

   La definizione del processo Gestione Cambiamento viene visualizzata in CA Workflow.

2. Fare clic con il pulsante sinistro del mouse su qualsiasi nodo che contenga il simbolo più (+) e selezionare Apri scheda o Apri in linea.

   I dettagli della sotto-attività vengono visualizzati in una nuova scheda o vicino alle attività della definizione del processo.

Modalità per l'impostazione dell'invio di notifiche per posta elettronica ai contatti di Gestione Cambiamento

Il sistema invia per posta elettronica notifiche sulle assegnazioni delle attività relative all'ordine di cambiamento e sulle modifiche apportate allo stato. Le notifiche inviate per posta elettronica contengono collegamenti all'elenco di lavoro o all'ordine di cambiamento utilizzabili per ulteriori revisioni. Poiché la definizione del processo Gestione cambiamento invia notifiche per posta elettronica, è necessario configurare un programma di posta.

Per impostare l'invio di notifiche per posta elettronica ai contatti di Gestione Cambiamento, effettuare le seguenti operazioni:

1. Nella scheda Amministrazione selezionare Gestione opzioni, Opzioni di posta elettronica.

   Viene visualizzato l'Elenco opzioni.

2. Configurare le opzioni di posta elettronica appropriate per la propria organizzazione.

Nota: per informazioni sulla configurazione della posta elettronica, consultare la *Guida in linea*.

Modalità per la creazione di gruppi per il processo Gestione Cambiamento

Quando si creano gruppi responsabili delle approvazioni e di altre attività per il processo Gestione Cambiamento, tenere presente quanto segue:

- È possibile usare qualsiasi nome di gruppo, a condizione che i nomi di CA SDM e CA EEM corrispondano.
- Il nome del gruppo in CA SDM deve corrispondere anche al nome della cartella del gruppo CA EEM.
- Ciascun gruppo deve contenere più di un membro.
- I membri del gruppo devono corrispondere sia in CA SDM che in CA EEM. Ad esempio, se il gruppo CAB di CA SDM ha quattro membri, anche il gruppo CAB di CA EEM deve avere lo stesso numero di membri.

Nota: per informazioni su come creare gruppi CA SDM e CA EEM, consultare la *Guida in linea* e la documentazione di CA EEM.

Per creare gruppi per il processo Gestione Cambiamento, effettuare le seguenti operazioni:

1. Nella scheda Amministrazione, selezionare Gestione protezione e ruoli, Gruppi.

   Viene visualizzata la pagina Ricerca gruppo.

2. Fare clic su Crea nuovo.

   Viene visualizzata la pagina Crea nuovo gruppo.

3. Creare i seguenti gruppi in CA SDM:

   - **Gruppo CAB**—Un gruppo CAB associato alla categoria cambiamento o all'ordine di cambiamento.
   - **Gruppo Implementazione**—Un gruppo di implementazione che è assegnato alla categoria cambiamento o all'ordine di cambiamento.

4. Fare clic su Salva.

   Viene visualizzata la pagina Dettagli gruppo.

5. Creare gli stessi gruppi in CA EEM.

Ulteriori informazioni:

Gestione dei gruppi CAB (a pagina 847)
Assegnazione dei gruppi CAB (a pagina 849)

Modalità per la creazione di contatti per il processo Gestione Cambiamento

Quando utilizza la definizione del processo Gestione Cambiamento, è possibile creare i contatti responsabili delle approvazioni e di altre attività durante il processo di cambiamento. È necessario anche assegnare i contatti ai gruppi del processo Gestione Cambiamento (a pagina 827).

Per creare contatti per il processo Gestione Cambiamento, effettuare le seguenti operazioni:

1. Nella scheda Amministrazione, selezionare Gestione protezione e ruoli, Contatti.

   Viene visualizzata la pagina Ricerca contatto.

2. Fare clic su Crea nuovo.

   Viene visualizzata la pagina Crea nuovo contatto.

3. Creare i seguenti contatti con indirizzi di posta elettronica validi e assegnarli ai gruppi appropriati:

   - **Richiedente—**Uno o più contatti che inviano la richiesta di cambiamento.
   - **Gestore cambiamento**—Contatto che rappresenta il manager del gruppo Implementazione. È possibile impostare un solo gestore cambiamento per il gruppo Implementazione.
   - **Gestore CAB**—Contatto che rappresenta il manager del gruppo CAB. È possibile impostare un solo gestore CAB per il gruppo CAB.

   La scheda dei gruppi dei dettagli dei contatti elenca le assegnazioni correnti del gruppo.

4. Nella scheda Membri della pagina dei dettagli del gruppo Implementazione, impostare il flag Gestione per Gestore cambiamento e Gestore CAB.

5. Fare clic su Salva.

   La scheda Membri visualizza Gestore-Sì per i seguenti contatti:

   - Gestore cambiamento
   - Gestore CAB

6. Creare gli stessi contatti in CA EEM e assegnarli ai gruppi CA EEM.

Nota: per i nomi dei contatti, è possibile usare qualsiasi nome utente valido o per l'accesso al sistema. Per informazioni su come creare contatti CA SDM e CA EEM, consultare la *Guida in linea* e la documentazione di CA EEM.

Impostazione di una porta alternativa per il server Tomcat di CA Workflow

Se il server Tomcat di CA Workflow è in esecuzione su una porta diversa dalla porta predefinita 8090, è necessario configurare la porta che CA Workflow dovrà utilizzare per comunicare con CA SDM.

Per impostare una porta alternativa per il server Tomcat di CA Workflow:

1. Aprire l'applicazione CA Workflow.

   Viene visualizzata la pagina di CA Workflow.

2. Fare clic sulla scheda Attori.

   Viene visualizzato l'elenco dei tipi di attore/attori.

3. Selezionare JavaScript, USD_Initializer.

   Viene visualizzata la pagina Opzioni attività di CA Workflow.

4. Fare doppio clic su Ottieni attributi globali.

   Viene visualizzata la pagina Funzionamento JavaScript.

5. Modificare il valore di WFTomcatPort su quello della nuova porta usata dal server Tomcat di CA Workflow.

6. Fare clic su OK.

   Il server Tomcat Server viene configurato per consentire a CA Workflow di comunicare con CA SDM.

Configurazione di una categoria cambiamento

Quando si specifica una categoria cambiamento per la definizione del processo Gestione Cambiamento, ogni nuovo ordine di cambiamento che utilizza la categoria avvia automaticamente la definizione del processo Gestione Cambiamento. L'ordine di cambiamento viene automaticamente compilato con tutti i valori della categoria cambiamento preconfigurati.

Per configurare una categoria cambiamento:

1. Nella scheda Amministrazione, selezionare Service Desk Manager, Ordini di cambiamento, Categorie.

   Viene visualizzato l'Elenco categorie cambiamento.

2. Creare o aprire una categoria cambiamento.

   Viene visualizzata la pagina Dettagli categoria cambiamento.

3. Nella scheda Workflow fare clic su CA Workflow.

4. Fare clic sul collegamento Definizione CA Workflow.

   Viene visualizzato l'Elenco Definizioni CA Workflow.

5. Fare clic su Gestione Cambiamento - Service Desk r12,1.

6. Fare clic su OK.

   Viene visualizzata la pagina Dettagli categoria cambiamento.

7. (Facoltativo) Assegnare il CAB, gruppo e indagine del rischio.

8. Fare clic su Salva.

   L'ordine di cambiamento successivo che utilizza la categoria avvia automaticamente la definizione del processo Gestione Cambiamento utilizzando i valori specificati nella categoria cambiamento.

Nota: per informazioni sulla creazione o la modifica dei categoria cambiamento, consultare la *Guida in linea*.

Installazione dell'opzione Category_Defaults in Gestione opzioni

L'opzione Category_Defaults utilizza i campi di categoria per inserire dati nell'indagine di rischio, di gruppo e CAB nell'ordine di cambiamento. Ad esempio, il gruppo CAB specificato per una categoria è presente in tutti i nuovi ordini di cambiamento che utilizzano la categoria.

Per installare l'opzione Category_Defaults in Gestione opzioni

1. Nella scheda Amministrazione selezionare Gestione ordini di cambiamento, Category_Defaults.

   Viene visualizzato l'Elenco opzioni.

2. Fare clic con il pulsante destro del mouse su Modifica Category_Defaults.

   Viene visualizzata la pagina delle opzioni di aggiornamento di Category_Defaults.

3. Fare clic su Installa.

4. Riavviare i servizi CA SDM.

   I nuovi ordini di cambiamento includeranno automaticamente i valori della categoria.

Funzionamento della definizione del processo Gestione Cambiamento

Quando un richiedente salva un Ordine di cambiamento contenente una categoria che utilizza la definizione del processo Gestione Cambiamento, viene automaticamente aperta la definizione.

Le sezioni che seguono spiegano come funziona la definizione del processo Gestione Cambiamento in CA SDM:

1. Il richiedente apre e salva l'Ordine di cambiamento che comprende le seguenti informazioni:

   Richiedente

   Identifica la persona che ha aperto l'Ordine di cambiamento.

   Categoria Cambiamento

   Identifica la categoria dell'Ordine di cambiamento.

   Tipo

   Identifica il tipo di Ordine di cambiamento, ad esempio Standard, Normale o Cambiamenti urgenti. Il tipo viene talvolta aggiornato durante l'uso del processo Workflow.

   Riepilogo/Descrizione

   Descrive il motivo per cui è stato richiesto un Ordine di cambiamento.

   Data di inizio pianificata

   Mostra la data di inizio.

   Durata

   Indica la durata stimata per il Cambiamento.

   Elementi configurazione

   Identifica almeno uno degli elementi della configurazione interessati.

   La definizione del processo Gestione Cambiamento si avvia. Il richiedente riceve una notifica per posta elettronica che lo informa che è necessario completare l'indagine di valutazione del rischio.

2. Il richiedente esamina l'Ordine di cambiamento e completa l'indagine di valutazione del rischio (a pagina 838) che descrive in che misura l'Ordine di cambiamento ha effetto sui server, le applicazioni e gli utenti.

   La definizione del processo Gestione Cambiamento analizza le risposte per determinare il rischio e verificare che l'Ordine di cambiamento segua il percorso di elaborazione appropriato. Il richiedente riceve per posta elettronica una notifica che lo informa che è necessario effettuare l'analisi dei conflitti e dell'impatto.

3. Durante l'analisi dei conflitti e dell'impatto (a pagina 839), il richiedente verifica che non ci siano conflitti a livello di pianificazione e analizza l'impatto dell'Ordine di cambiamento sugli elementi della configurazione.

   Il richiedente riceve per posta elettronica una notifica che lo informa che è necessario effettuare l'analisi del Cambiamento.

4. Durante l'analisi del Cambiamento (a pagina 840), il richiedente identifica e invia il tipo di Cambiamento, il motivo del Cambiamento, l'impatto sul business e l'impatto generale del Cambiamento.

   Il gestore del Cambiamento riceve per posta elettronica una notifica che lo informa che è necessario approvare l'Ordine di cambiamento. Se l'Ordine di cambiamento ha un rischio elevato, viene inviata una notifica anche al gruppo CAB.

5. La gestione del Cambiamento rivede l'analisi del Cambiamento e inserisce commenti sulla revisione. La gestione del Cambiamento approva, rifiuta o contrassegna l'Ordine di cambiamento come Incompleto (a pagina 839).

   Il sistema aggiorna di conseguenza la pagina Dettagli Ordine di cambiamento e risponde effettuando una delle seguenti azioni:

   - Se l'Ordine di cambiamento viene approvato e non è necessaria l'approvazione CAB, il sistema invia una notifica al gruppo di implementazione. L'Ordine di cambiamento visualizza lo stato Approvato.
   - Se l'Ordine di cambiamento viene approvato, ma sono necessarie ulteriori approvazioni CAB, viene inviata una notifica al gestore e ai membri CAB per l'approvazione. L'Ordine di cambiamento visualizza lo stato Approvazione in corso.
   - Se l'Ordine di cambiamento viene rifiutato, visualizza lo stato Rifiutato.
   - Se l'Ordine di cambiamento viene contrassegnato come incompleto, visualizza lo stato Incompleto.

6. Per gli Ordine di cambiamento approvati, un membro del gruppo di implementazione conferma l'avvio dell'implementazione (a pagina 843) e attua il Cambiamento.

   L'Ordine di cambiamento visualizza lo stato Implementazione in corso.

7. Quando il lavoro è terminato, il gestore del gruppo di implementazione completa la revisione post-implementazione (a pagina 845) (PIR) fornendo dettagli sul risultato del Cambiamento.

   CA Workflow chiude l'Ordine di cambiamento. L'Ordine di cambiamento visualizza un codice di chiusura e lo stato Implementato.

Ulteriori informazioni:

Visualizzazione delle indagini di rischio predefinite (a pagina 853)
Modalità di implementazione di un'indagine di rischio (a pagina 852)
Come configurare la definizione dei processi di gestione dei cambiamenti (a pagina 824)

Modalità di gestione delle approvazioni degli ordini di cambiamento nella definizione dei processi di gestione dei cambiamenti

Nel diagramma che segue viene mostrato come la definizione dei processi di gestione dei cambiamenti (a pagina 831) gestisce le approvazioni per un nuovo ordine di cambiamento.

Azione utente
Definizione del processo di gestione del Cambiamento
Inizio
Il richiedente crea l'Ordine di cambiamento
Notifica di completamento dell'analisi Cambiamento al richiedente
Il richiedente completa la valutazione del rischio
Impostazione stato = RFC
Notifica di completamento dell'analisi Impatto+Conflitto al richiedente
Il richiedente completa l'analisi di impatto e conflitto
Notifica di completamento dell'analisi del Cambiamento al richiedente
Il richiedente esegue l'analisi del Cambiamento
Aggiornamento del tipo di Cambiamento, Rischio e Business Case
Tipo Cambiamento?
2. Tipo Camb. =Standard
1. Tipo Camb.= Rischio normale, alto-estremo
4. Tipo Camb.=Normale, Medio-Basso
3. Tipo Camb.=Emergenza
Impostazione flag approvazione CAB=No
Impostazione flag approvazione CAB=No
Impostazione flag approvazione CAB=Sì
Invio notifica ECAB
Impostazione stato = Applicazione in corso
Notifica Manager Cambiamento per l'approvazione
Il manager del Cambiamento approva l'Ordine di Cambiamento
1. Sì. Approvazione CAB non richiesta
2. Sì. Approvazione CAB richiesta
Recupero CAB + Notifica di approvazione
Notifica gruppo implementazione per il completamento Ordine di cambiamento
Approvato?
3. Respinto
Impost. Stato= Notifica richiedente-Respinto, Rielaborazione gruppo implementazione
4.Incompleto
Impost. Stato= Notifica richiedente-Incompleto
Continua

Modalità di gestione delle implementazioni degli ordini di cambiamento nella definizione dei processi di gestione dei cambiamenti

Nel diagramma che segue viene mostrato come la definizione dei processi di gestione dei cambiamenti (a pagina 831) gestisce l'implementazione degli ordini di cambiamento.

Implementazione Ordine di cambiamento
Azione utente
Definizione processo Gestione Cambiamento
Input: Ordine di cambiamento approvato
Continua
Implementato?
Sì
No
Stato = Implementazione completata Chiusura codice = Corretta
Notifica richiedente
Notifica Gruppo Implementazione per ritiro Cambiamento
Stato = Ritirato Chiusura codice = Errore
Notifica Gruppo Implementazione per verifica del ritiro
Ritirato?
Errore
Notifica richiedente Crea Incidente
Rimanda PIR
Correttamente
Notifica richiedente
Notifica gruppo
Gruppo Implementazione completa PIR
Chiusura Ordine di cambiamento
STOP

Completamento di un'indagine di valutazione del rischio

Quando si crea un ordine di cambiamento, il sistema invia una notifica per segnalare che è necessario completare l'indagine di valutazione del rischio associata alla categoria cambiamento. Il richiedente dovrà identificare, valutare e quantificare i rischi degli ordini di cambiamento che appartengono alle categorie cambiamento prima di modificare un sistema o servizio.

Per completare un'indagine di valutazione del rischio:

1. Aprire l'ordine di cambiamento facendo clic sul collegamento relativo all'indagine di valutazione del rischio contenuto nella notifica ricevuta per posta elettronica.

   Viene visualizzata la pagina Dettagli ordine di cambiamento.

2. Nella scheda Attività Workflow, fare clic sul collegamento relativo all'indagine di valutazione del rischio del richiedente e seguire le istruzioni per completare l'indagine.

   Viene visualizzato l'elenco CA Workflow.

3. Nella scheda Attività fare clic sul collegamento Esegui.

   Viene visualizzata la pagina Esegui attività.

4. Prendere nota delle istruzioni e fare clic sul collegamento.

   Si apre l'indagine di rischio.

5. Rispondere attentamente alle domande dell'indagine in modo che il workflow del processo Gestione Cambiamento possa valutare attentamente il percorso di rischio appropriato per il cambiamento.

6. Fare clic su Invia.

   Viene visualizzata la pagina Esegui attività.

7. Fare clic su Conferma.

   La pagina Dettagli ordine di cambiamento visualizza Stato-RFC. Il richiedente riceve per posta elettronica una notifica che lo informa che è necessario effettuare l'analisi dei conflitti e dell'impatto.

Ulteriori informazioni:

Modalità di accesso a un'indagine di rischio direttamente da un URL (a pagina 854)

Esecuzione dell'analisi dei conflitti e dell'impatto

Durante l'analisi dei conflitti e dell'impatto, il richiedente verifica che non ci siano conflitti a livello di pianificazione e analizza l'impatto dell'ordine di cambiamento sugli elementi della configurazione.

Per eseguire l'analisi dei conflitti e dell'impatto:

1. Aprire l'ordine di cambiamento facendo clic sul collegamento contenuto nella notifica ricevuta per posta elettronica.

   Viene visualizzata la pagina Dettagli ordine di cambiamento.

2. Nella scheda Attività Workflow, fare clic sul collegamento Impatto richiedente e Analisi conflitti.

   Viene visualizzata la pagina Attività.

3. Nella scheda Attività fare clic sul collegamento Esegui.

   Viene visualizzata la pagina Esegui attività.

4. Prendere nota delle istruzioni per l'analisi dell'impatto e dei conflitti e fare clic sul collegamento.

   Viene visualizzata la pagina Dettagli ordine di cambiamento.

5. Nella scheda Conflitti ordine di cambiamento fare clic su Analisi conflitti per risolvere tutti i conflitti relativi alla pianificazione e pendenti. Risolvere tutti i conflitti prima di implementare la modifica.

   Viene visualizzato l'elenco dei conflitti.

6. Nella scheda Elementi config fare clic su Analisi impatto per rivedere i dettagli relativi agli elementi della configurazione.

   Viene visualizzato l'Elenco elementi della configurazione.

7. Nella scheda Elementi della configurazione Nella scheda Elementi fare clic su Impact Explorer per rivedere le informazioni relative a ciascun elemento della configurazione.

   Impact Explorer si apre.

8. Fare clic su Visualizzatore per visualizzare le relazioni degli elementi della configurazione in formato grafico.

   Nota: il pulsante Visualizzatore è disponibile solo se CA CMDB è installato.

9. Tornare alla pagina Esegui attività e fare clic su Conferma.

   La scheda Attività Workflow visualizza un collegamento che consente di avviare l'analisi del cambiamento. Il richiedente riceve per posta elettronica una notifica che lo informa che è necessario effettuare l'analisi del cambiamento.

Ulteriori informazioni:

Impact Explorer (a pagina 855)
Avvio di CMDB Visualizer da Impact Explorer (a pagina 858)

Esecuzione di un'analisi del cambiamento

Durante l'analisi del cambiamento, il richiedente identifica e registra le seguenti informazioni:

- Tipo di cambiamento
- Motivo del cambiamento
- Impatto sul business
- Impatto generale della modifica

Per eseguire un'analisi del cambiamento:

1. Aprire l'ordine di cambiamento facendo clic sul collegamento contenuto nella notifica ricevuta per posta elettronica.

   Viene visualizzata la pagina Dettagli ordine di cambiamento.

2. Nella scheda Attività Workflow fare clic sul collegamento del modulo relativo all'analisi del cambiamento richiedente.

   Viene visualizzata la pagina Attività.

3. Nella scheda Attività fare clic sul collegamento Esegui.

   Viene visualizzata la pagina Analisi cambiamento.

4. Nella scheda Analisi mod rispondere a tutte le domande per confermare l'ordine di cambiamento e fare clic su Invia. Ad esempio, è possibile fornire un riepilogo della propria analisi e spiegare lo scopo per cui viene richiesto un ordine di cambiamento. se necessario, specificare se l'ordine di cambiamento è una ripetizione o rilavorazione. Riepilogare l'impatto sul business e l'impatto generale del cambiamento.

   A seconda del tipo di cambiamento e del rischio, il sistema effettua le seguenti operazioni:

   - Se il tipo di cambiamento è Normale e il rischio è alto-molto alto, la pagina Dettaglio ordine di cambiamento visualizza le seguenti informazioni:
     - Approvazione CAB-Sì
     - Stato-Approvazione in corso

     Il sistema invia al gestore del cambiamento una notifica per segnalargli di approvare l'ordine di cambiamento. Appena il gestore approva il cambiamento, viene inviata una notifica al gruppo CAB per richiedere un'ulteriore approvazione.

- Se il tipo di cambiamento è Normale e il rischio è alto-basso, la pagina Dettaglio ordine di cambiamento visualizza le seguenti informazioni:
  - Approvazione CAB-No
  - Stato-Approvazione in corso

  Il sistema invia al gestore del cambiamento una notifica per segnalargli di approvare l'ordine di cambiamento.
- Se il tipo di cambiamento è Standard, il sistema invia una notifica al gruppo di implementazione per segnalargli di implementare il cambiamento.
- Se il tipo di cambiamento è Emergenza, la pagina Dettagli ordine di cambiamento visualizza Approvazione CAB-No.

  Il sistema invia una notifica a ECAB. Appena ECAB ha elaborato l'ordine di cambiamento, la pagina Dettagli ordine di cambiamento visualizza Stato-Approvazione in corso e il gestore del cambiamento riceve una notifica che lo informa che deve approvare l'ordine di cambiamento.

Approvazione, rifiuto o impostazione di un ordine di cambiamento come incompleto

Il tipo di ordine di cambiamento e il livello di rischio influenzano il processo di approvazione per gli ordini di cambiamento che utilizzano la definizione del processo Gestione Cambiamento. I seguenti valori dell'ordine di cambiamento determinano gli approvatori degli ordini di cambiamento:

- Se il tipo è Normale e il rischio è Medio-basso, l'ordine di cambiamento deve essere approvato da un solo gestore del cambiamento.
- Se il tipo è Normale e il rischio è Alto-molto alto, l'ordine di cambiamento deve essere approvato da un membro del gruppo CAB.
- Se il tipo è Standard, non sono necessarie approvazioni. Il sistema invia una notifica al gruppo di implementazione per segnalargli di intervenire sull'ordine di cambiamento.
- Se il tipo è Emergenza, il sistema invia una notifica al gruppo ECAB. L'ordine di cambiamento visualizza Stato-Approvazione in corso. Quando l'ordine di cambiamento è pronto per l'approvazione, il sistema invia una notifica al gestore del cambiamento.

Il revisore esamina le informazioni dell'analisi dei cambiamenti e stabilisce se approvare o rifiutare l'ordine di cambiamento oppure contrassegnarlo come non completo.

Per approvare o rifiutare un ordine di cambiamento o contrassegnarlo come non completo

1. Aprire l'ordine di cambiamento facendo clic sul collegamento di notifica di posta elettronica.

   Viene visualizzata la pagina Dettagli ordine di cambiamento.

2. Nella scheda Attività flusso di lavoro fare clic sul collegamento del modulo di approvazione di Gestione cambiamento.

   Viene visualizzata la pagina Attività.

3. Nella scheda Attività fare clic sul collegamento Esegui.

   Viene visualizzata la pagina relativa all'approvazione di Gestione cambiamento o CAB.

4. Esaminare la scheda relativa all'analisi del cambiamento per ottenere informazioni aggiuntive sull'ordine di cambiamento.

5. In base al livello di approvazione richiesto, selezionare una delle seguenti schede di approvazione e rispondere alle domande di approvazione:

   Approvazione di Gestione cambiamento

   Descrive la decisione del gestore cambiamenti relativamente all'ordine di cambiamento.

   Approvazione CAB

   Descrive la decisione del revisore CAB relativamente all'ordine di cambiamento.

6. Scegliere uno dei seguenti livelli di approvazione:

   Approva

   Accetta l'ordine di cambiamento.

   Rifiuta

   Rifiuta l'ordine di cambiamento.

   Non completo

   Contrassegna l'ordine di cambiamento come non completo.

   Viene visualizzata la pagina Risultato. A seconda del livello di approvazione, si verificano le seguenti azioni:

   - Se si approva l'ordine di cambiamento e non è richiesta un'approvazione CAB aggiuntiva, nella pagina Dettagli ordine di cambiamento viene visualizzato lo stato Approvato e il gruppo implementazione viene informato che deve iniziare a lavorare.
   - Se si approva l'ordine di cambiamento ed è richiesta l'approvazione CAB, nella pagina Dettagli ordine di cambiamento viene visualizzato lo stato Approvazione in corso. Viene informato anche il gruppo CAB.
   - Se si rifiuta l'ordine di cambiamento, nella pagina Dettagli ordine di cambiamento viene visualizzato lo stato Rifiutato e il richiedente e il gruppo di implementazione ricevono una notifica.
   - Se l'ordine di cambiamento non è completo, nella pagina Dettagli ordine di cambiamento viene visualizzato lo stato Non completo e il richiedente riceve una notifica.

Ulteriori informazioni:

Modalità di funzionamento del processo CAB (a pagina 791)
Approvazioni CAB (a pagina 849)
Responsabilità del gruppo CAB (a pagina 790)

Implementazione di un Ordine di cambiamento

Per un Ordine di cambiamento specifico, un gruppo di implementazione completa uno o più elementi di lavoro. I membri del gruppo di implementazione, creano un report delle informazioni sul Cambiamento.

Procedere come descritto di seguito:

1. Accedere a CA SDM come membro del gruppo di implementazione e aprire l'Ordine di cambiamento.

   Viene visualizzata la pagina Dettagli Ordine di Cambiamento.

2. Nella scheda Ulteriori informazioni, Attività del flusso di lavoro fare clic sul collegamento Implement Change Order (Implementa Ordine di cambiamento).

   Viene visualizzata la pagina Elenco Attività.

3. Nella scheda Attività fare clic sul collegamento Esegui.

   Viene visualizzata la pagina per l'esecuzione delle attività.

4. Attenersi alle istruzioni per la revisione dell'Ordine di cambiamento e fare clic su Conferma.

   Nella pagina Dettagli Ordine di cambiamento viene mostrato lo stato Implementazione in corso.

5. Implementazione del Cambiamento. Ad esempio, se nell'Ordine di cambiamento è stato indicato di installare la patch AntiVirus in Exchange Server 1 ed Exchange Server 2, completare l'Ordine di cambiamento in base alle linee guida e agli standard dell'azienda.

6. Nella scheda Attività del flusso di lavoro fare clic sul collegamento per l'implementazione del modulo completato.

   Viene visualizzata la pagina Attività.

7. Nella scheda Attività fare clic sul collegamento Esegui.

   Viene visualizzata la pagina per il completamento dell'implementazione.

8. Nella scheda relativa al completamento dell'implementazione rispondere alle domande per descrivere il modo in cui il proprio gruppo ha implementato l'Ordine di cambiamento e fare clic su una delle seguenti opzioni:

   Completa

   Specifica che tutte le attività relative all'Ordine di cambiamento sono state completate. Imposta lo stato dell'Ordine di cambiamento sull'opzione che indica che l'implementazione è completa e imposta Codice di chiusura su Riuscito.

   Non completo

   Specifica che non è stato possibile completare uno o più elementi nell'Ordine di cambiamento.

   Il richiedente riceve una o più notifiche relative al completamento o al ritiro dell'Ordine di cambiamento. Il sistema risponde in uno dei seguenti modi:

   - Se l'Ordine di cambiamento è completo, nella pagina Dettagli Ordine di cambiamento viene visualizzato quanto segue:
     - Stato: Implementazione completa
     - Codice di chiusura: Riuscito.

     Il sistema informa il gruppo di implementazione che deve completare la revisione post implementazione.

   - Se l'Ordine di cambiamento non è completo, nella pagina Dettagli Ordine di cambiamento viene visualizzato quanto segue:
     - Stato: Ritirato
     - Codice di chiusura: Non riuscito.

     Il sistema informa inoltre il gruppo di implementazione che deve stabilire se il ritiro è riuscito.

     Se il ritiro è stato completato correttamente, il sistema informa il gruppo di implementazione che deve completare la revisione post implementazione. Se il ritiro non è stato completato correttamente, il sistema crea un Incidente e informa il gruppo di implementazione che deve completare la revisione post implementazione.

Completamento della revisione post-implementazione

Al termine di un lavoro, il gruppo di implementazione completa il modulo di revisione post-implementazione (PIR) che descrive il risultato del cambiamento. I membri del gruppo di implementazione completano generalmente il modulo PIR in tre-sette giorni dopo l'implementazione dell'ordine di cambiamento. Tuttavia, la definizione del processo Gestione Cambiamento imposta un ritardo predefinito di dieci secondi per l'assegnazione di questa attività.

Per completare la revisione post-implementazione:

1. Accedere a CA SDM come membro del gruppo di implementazione e aprire l'ordine di cambiamento.

   Viene visualizzata la pagina Dettagli ordine di cambiamento.

2. Nella scheda Attività Workflow fare clic sul collegamento relativo alla revisione post-implementazione.

   Viene visualizzato l'elenco delle attività.

3. Nella scheda Attività fare clic sul collegamento Esegui.

   Viene visualizzata la pagina PIR.

4. Nella scheda PIR rispondere alle domande per descrivere la risoluzione e fare clic su Invia.

   La pagina Dettagli ordine cambiamento visualizza Stato-Chiuso.

Attore ActivityNode non trovato: Aggiorna oggetto -Service Desk r12

Sintomo:

La finestra del comando CA Workflow visualizza il seguente errore:

```
Attore ActivityNode non trovato: Aggiorna oggetto -Service Desk r12
```

Soluzione:

1. Accedere all'applicazione CA Workflow.
2. Fare clic sulla scheda Attori.
3. Selezionare la cartella Processi.
4. Selezionare File/Nuovo attore.
5. Selezionare Aggiorna oggetto –Service Desk r12 dall'elenco a discesa.
6. Fare clic su OK.

   Il sistema utilizza il nuovo attore nella definizione del processo Gestione Cambiamento.

L'ordine di cambiamento non si chiude

Sintomo:

L'ordine di cambiamento non si chiude durante l'ultima fase del flusso di lavoro. L'istanza del processo CA Workflow visualizza lo stato In esecuzione e i report CA Workflow come un errore relativo a un guasto dell'attore.

Soluzione:

Quando si chiude un ordine di cambiamento, verificare di aver impostato tutti i campi obbligatori, come Causa principale.

Console CAB e reporting

La console CAB è un dashboard che semplifica e velocizza l'approvazione online di ordini di cambiamento che richiedono l'approvazione CAB. Gestione cambiamenti e gli altri membri del gruppo CAB utilizzano la console per visualizzare i dettagli di un ordine di cambiamento, oltre alle attività flusso di lavoro ed elementi della configurazione associati, e per approvare o rifiutare l'ordine di cambiamento. La console CAB consente ai membri del team di analizzare, approvare o rifiutare un ordine di cambiamento, per poi passare rapidamente al successivo ordine di cambiamento. Nel caso di una richiesta di ordine di cambiamento, il gruppo CAB può soddisfarla direttamente o eseguirne l'escalation a un gruppo appropriato.

Gestione cambiamenti può utilizzare le opzioni incorporate di CA SDM per riepilogo e dettagli al fine di effettuare quanto segue:

- Segnalare gli ordini di cambiamento approvati e rifiutati
- Segnalare gli ordini di cambiamento in attesa di approvazione

Per stampare o visualizzare i report di riepilogo e dei dettagli, per prima cosa è necessario selezionare i record da includere nel report. È possibile selezionare record specifici per un report utilizzando la funzione di ricerca delle pagine di elenco.

Ad esempio, nell'Elenco ordini di cambiamento è possibile immettere criteri di ricerca per creare un elenco di ordini di cambiamento da utilizzare per la creazione di un report.

Nota: per ulteriori informazioni sulla creazione di report di riepilogo e dettagli in CA SDM, vedere le informazioni sulla generazione dei report nella *Guida in linea*.

Ulteriori informazioni:

Gestione dei gruppi CAB (a pagina 847)
Assegnazione dei gruppi CAB (a pagina 849)
Approvazioni CAB (a pagina 849)
Cambiamento delle proprietà della console CAB (a pagina 849)
Funzionalità di reporting del ruolo Gestione cambiamento (a pagina 851)

Gestione dei gruppi CAB

È possibile creare e gestire gruppi CAB con membri appropriati per gli ordini di cambiamento presi in considerazione. Il gruppo CAB può contenere membri del team delle applicazioni, un responsabile dello sviluppo, un proprietario di componenti, personale di QA e supporto e qualsiasi altra persona che si ritenga necessaria.

Nota: prima di implementare un gruppo CAB, configurare i contatti appropriati per la propria struttura aziendale.

Per creare un gruppo CAB

1. Nella scheda Amministrazione, selezionare Gruppi.

   Viene visualizzata la pagina Ricerca gruppo.

2. Fare clic su Crea nuovo.

   Viene visualizzata la pagina Crea nuovo gruppo.

3. Completare i campi in modo appropriato.

4. Fare clic su Salva.

   Il gruppo CAB viene visualizzato nella pagina Elenco gruppi.

Per assegnare i membri al gruppo CAB

1. Selezionare la scheda Membri nella pagina Dettagli gruppo.

2. Fare clic su Aggiorna membri.

   Viene visualizzata la pagina Ricerca contatto.

3. Immettere i criteri di ricerca per visualizzare i contatti desiderati e fare clic su Cerca.

   Viene visualizzata la pagina Aggiornamento membri, che elenca i contatti corrispondenti ai criteri di ricerca.

4. Scegliere dall'elenco di sinistra i contatti da assegnare al gruppo. Per selezionare più elementi, tenere premuto il tasto Ctrl mentre si fa clic con il pulsante sinistro del mouse.

5. Una volta selezionati tutti i contatti desiderati, fare clic sul pulsante di selezione (>>).

   I contatti selezionati vengono spostati nell'elenco Membri sulla destra.

6. Fare clic su OK.

   Viene visualizzata la pagina Dettagli gruppo. I contatti selezionati sono elencati nella scheda Membri.

Per aggiungere il gruppo CAB a una categoria di cambiamento

Nota: assicurarsi che l'opzione Category_Defaults sia installata, in modo che il campo CAB negli ordini di cambiamento venga impostato automaticamente su un gruppo CAB.

1. Nella scheda Amministrazione, selezionare CA SDM, Ordini di cambiamento, Categorie.

   Viene visualizzato l'Elenco categorie cambiamento.

2. Selezionare una categoria dall'elenco.

   Viene visualizzata la pagina Aggiorna categoria cambiamento.

3. Selezionare il gruppo CAB appropriato dal campo CAB.
4. Compilare gli altri campi in modo appropriato.
5. Fare clic su Salva.

   Nella pagina Dettagli categoria cambiamento viene visualizzato un messaggio relativo a un salvataggio eseguito correttamente.

6. Fare clic su Chiudi finestra.

   Il gruppo CAB viene associato alla categoria e all'ordine di cambiamento.

Ulteriori informazioni:

Area_Defaults (a pagina 494)
Categorie Ordine di cambiamento e Issue (a pagina 411)

Assegnazione dei gruppi CAB

È possibile assegnare un gruppo di CAB per analizzare un ordine di cambiamento prima che venga implementato.

Per assegnare un gruppo CAB a un ordine di cambiamento

1. Selezionare l'ordine di cambiamento desiderato dall'Elenco ordini di cambiamento.

   Viene visualizzata la pagina Dettagli ordine di cambiamento.

2. Fare clic su Modifica.
3. Selezionare CAB nell'area Dettagli.

   Viene visualizzata la pagina con l'elenco dei gruppi.

4. Selezionare un gruppo CAB.
5. Fare clic su Salva e chiudere la finestra.

   Il gruppo CAB è assegnato all'ordine di cambiamento.

Approvazioni CAB

Se il campo Approvazione CAB è impostato su SÌ, Il gruppo CAB (Change Advisory Board) deve approvare un ordine di cambiamento prima che venga implementato. Durante il processo di approvazione, se il gestore cambiamenti fa clic su Approva o Rifiuta, lo stato dell'ordine di cambiamento diventa, rispettivamente, Approvato o Rifiutato.

Nota: se si desidera utilizzare valori di stato diversi, è possibile aggiornare il codice del pulsante Approva o Rifiuta mediante Web Screen Painter.

Ulteriori informazioni:

Cambiamento delle proprietà della console CAB (a pagina 849)

Cambiamento delle proprietà della console CAB

Utilizzando Web Screen Painter è possibile modificare le proprietà della console CAB che compaiono nei moduli Web. È possibile, ad esempio, effettuare le seguenti operazioni:

- Rinominare i pulsanti Approva e Rifiuta. Questi pulsanti sono proprietà nei moduli Web orderwf_approval_console.htmpl (attività CA Workflow) e order_approval_console.htmpl (ordini di cambiamento).

- Personalizzare i valori di stato dei pulsanti Approva e Rifiuta modificando i valori 'REJ' o 'APR'.
  - Il pulsante "Rifiuta attività" richiama una funzione approve_reject('REJ').
  - Il pulsante "Approva attività" richiama una funzione approve_reject('APR').

  Importante È possibile associare solo una transazione attiva a un pulsante. Non disattivare una transizione di stato predefinita associata a un pulsante, altrimenti smetterà di funzionare.

Per modificare le proprietà della console CAB

1. In Web Screen Painter aprire il modulo della console CAB da modificare.

   Web Screen Painter apre e visualizza il modulo.

2. Nella scheda Progetto, fare clic con il pulsante destro del mouse sul controllo da modificare, quindi selezionare Proprietà.

   Viene visualizzata la pagina Proprietà - *controllo*.

3. Modificare le proprietà desiderate immettendo un nuovo valore per ognuna di esse.

   Le modifiche diventano effettive non appena si fa clic all'esterno del campo o si chiude la pagina Proprietà.

   Web Screen Painter visualizza un breve riepilogo del significato di una proprietà in una nota che appare nella parte inferiore della finestra di dialogo Proprietà quando si seleziona la proprietà.

Nota: per informazioni su Web Screen Painter, consultare la *Guida all'implementazione*.

Esempio: personalizzazione della console CAB per le attività di flusso di lavoro cambiamento

Questo esempio mostra come personalizzare lo stato delle attività mediante Web Screen Painter.

1. In Web Screen Painter, aprire il modulo Web orderwf_approval_console.htmpl.

   Web Screen Painter apre e visualizza il modulo.

2. Nella scheda Progetto, fare clic con il pulsante destro del mouse sul pulsante Rifiuta attività e seleziona Proprietà.

   Viene aperta la pagina Proprietà - Pulsante.

3. Individuare la funzione approve_reject("REJ").

   "REJ" è il codice di stato per lo stato Reject dell'attività.

4. Immettere un nuovo valore per "REJ".

   Le modifiche diventano effettive non appena si fa clic all'esterno del campo o si chiude la pagina Proprietà.

   Web Screen Painter visualizza un breve riepilogo del significato di una proprietà in una nota che appare nella parte inferiore della finestra di dialogo Proprietà quando si seleziona la proprietà.

Funzionalità di reporting del ruolo Gestione cambiamento

Gestione cambiamenti con privilegi appropriati può utilizzare BusinessObjects InfoView per effettuare quanto segue:

- Segnalare il volume dei cambiamenti per sistema operativo, categoria di cambiamento, gruppo, implementatore, rischio, stato, data di implementazione, elementi della configurazione interessati e cambiamenti generati da ticket di incidente o problema.
- Segnalare cambiamenti implementati con successo raggruppati per categoria di cambiamento, urgenza, priorità, impatto, % di operazioni riuscite rispetto al totale per il periodo specificato e gruppo del richiedente del cambiamento.
- Segnalare cambiamenti non riusciti raggruppati per categoria, urgenza, priorità, impatto, motivo del ritiro, % di operazioni non riuscite rispetto al totale per il periodo specificato e gruppo del richiedente del cambiamento.
- Segnalare il numero totale di richieste di cambiamento per categoria di cambiamento, coordinatore dei cambiamenti, Gestione cambiamenti, livello di rischio, priorità ed elementi della configurazione interessati per un periodo specifico.

È possibile accedere ai report predefiniti nel riquadro sinistro della finestra InfoView per visualizzare, pianificare, modificare o eseguire il report desiderato, o per visualizzare la cronologia e le proprietà di un report.

Nota: per ulteriori informazioni sull'uso di BusinessObjects InfoView, vedere le informazioni su CA Business Intelligence nella *Guida in linea*.

Valutazione dei rischi

Le valutazioni dei rischi consentono di identificare, valutare e quantificare i rischi legati agli Ordini di cambiamento che appartengono a determinate categorie, prima di modificare un sistema o un servizio nell'ambiente. Per valutare i rischi si creano apposite indagini, da associare successivamente alle categorie di Cambiamento. Quando un utente crea un Ordine di cambiamento e specifica una categoria di Cambiamento, l'indagine associata alla categoria può essere completata e inviata.

L'indagine dei rischi elenca una serie di domande a scelta multipla o singola. Ogni risposta ha un peso. Quando si crea un Ordine di cambiamento, l'utente seleziona le risposte appropriate e invia l'indagine. Il livello di rischio valutato si basa sul peso delle risposte selezionate dall'utente.

Ulteriori informazioni:

Esempio di distribuzione di un'indagine di rischio (a pagina 853)
Visualizzazione delle indagini di rischio predefinite (a pagina 853)

Modalità di implementazione di un'indagine di rischio

Per implementare un'indagine di rischio, effettuare le seguenti operazioni:

1. Stabilire i livelli di rischio per la propria organizzazione.
2. Creare o selezionare un'indagine di rischio dall'elenco di indagini predefinite.
3. Creare o modificare le domande e le risposte dell'indagine di rischio.
4. Modificare gli intervalli di rischio per l'indagine.
5. Associare l'indagine di rischio a una categoria di cambiamento.
6. Dopo aver associato un'indagine di rischio a una categoria di Cambiamento, il pulsante Indagine di rischio viene visualizzato per il richiedente quando questi salva un Ordine di cambiamento utilizzando la categoria di Cambiamento specificata.
7. Visualizzare il rischio valutato in base ai risultati dell'indagine di rischio.
8. (Facoltativo) Ignorare il valore di rischio valutato dal menu Attività.

Nota: per informazioni dettagliate su come creare e modificare le indagini di rischio, vedere la *Guida in linea*.

Visualizzazione delle indagini di rischio predefinite

CA SDM dispone di indagini di rischio predefinite che è possibile associare alle categorie di cambiamento.

Per visualizzare le indagini di rischio predefinite

1. Accedere a Service Desk, Ordini di cambiamento, Indagine di rischio.
2. Selezionare General dalla colonna Nome indagine di rischio.

   Viene visualizzata la pagina General Risk Survey Detail.
3. Fare clic su Visualizza indagine.

   L'indagine di rischio che viene visualizzata elenca le domande, le risposte e il peso per ogni risposta. Questa indagine è valida per i cambiamenti generali all'interno dell'organizzazione.
4. Chiudere l'indagine.
5. Una volta visualizzata la pagina General Risk Survey Detail, chiuderla.

Esempio di distribuzione di un'indagine di rischio

Questo esempio dimostra come distribuire un'indagine di rischio predefinita sul sistema utilizzando una categoria di cambiamento predefinita.

1. Accedere a Service Desk, Ordini di cambiamento, Categorie.

   Viene visualizzato l'Elenco categorie cambiamento.
2. Selezionare Add.IT.Other dalla colonna Simbolo.

   Viene visualizzata la pagina dei dettagli della categoria Add.IT.Other.
3. Fare clic su Modifica.

   Viene visualizzata la pagina Categoria cambiamento aggiornamento Add.IT.Other Update.
4. Fare clic su Indagine di rischio.

   Viene visualizzata la pagina Cerca modello indagine di rischio.
5. Cercare l'indagine di rischio. In questo esempio, cercare Generale e selezionare l'indagine di rischio per aggiungerla al modulo dei dettagli.

   Nel campo Indagine di rischio compare la voce Generale.
6. Salvare e chiudere la finestra.

Se un utente crea un ordine di cambiamento utilizzando la categoria Add.IT.Other, il pulsante Indagine di rischio compare quando si salva l'ordine di cambiamento.

Modalità di accesso a un'indagine di rischio direttamente da un URL

È possibile fornire un URL dinamico per consentire a un utente di accedere a un'indagine di rischio per ordine di cambiamento direttamente attraverso un URL da un'attività in CA Workflow. È possibile aggiungere questo URL dinamico con il parametro *KEEP.UsingURL=1* per indicare che l'accesso all'indagine di rischio avviene direttamente con un URL.

Creare l'URL dinamico in CA Workflow come riportato di seguito:

1. Aprire la definizione di processo CA Workflow e aggiungere il nodo dell'attività per consentire a un utente di compilare l'indagine di rischio.
2. Nel nodo dell'attività, aggiungere un URL dinamico utilizzando la sintassi appropriata. Verificare di aggiungere il parametro *KEEP.UsingURL=1*, come riportato nell'esempio seguente:

   ```
   http://<nome host>:<porta>/CAisd/pdmweb.exe?CNT_ID=<ID del contatto>+CRID=<ID dell'ordine di cambiamento>+OP=DO_RISK_SURVEY+KEEP.UsingURL=1
   ```

   nome host

   Specifica il nome host del server applicazioni o l'URL di un'utilità di bilanciamento del carico per reindirizzare un insieme di server applicazioni.

   port

   Specifica la porta su cui è installato CA SDM.

   ID del contatto

   Specifica l'ID interno del contatto che compila l'indagine di rischio.

   ID dell'ordine di cambiamento

   Specifica l'ID interno dell'ordine di cambiamento associato all'indagine di rischio.

   Di seguito è riportato un esempio di URL:

   ```
   http://hostname:8080/CAisd/pdmweb.exe?CNT_ID=21A7CC606A3011DEA39AA8010000A800+CRID=400009+OP=DO_RISK_SURVEY+KEEP.UsingURL=1
   ```

   Importante: Se non si aggiunge il parametro *KEEP.UsingURL=1* all'URL dinamico, all'invio dell'indagine di rischio viene visualizzato un errore e non viene calcolato il livello di rischio.
3. Salvare la definizione di processo CA Workflow.
4. Creare una Categoria cambiamento e associarvi l'indagine di rischio e la definizione di processo CA Workflow.

   Salvare le modifiche.
5. Aprire un ordine di cambiamento con questa Categoria cambiamento e salvarlo per creare un'istanza del processo CA Workflow.

6. Nell'ambito del processo CA Workflow, a un utente viene assegnata un'attività per compilare l'indagine di rischio. L'utente fa clic sull'URL, come definito in precedenza.
7. L'utente accede a CA SDM utilizzando l'URL ed accede direttamente al contesto dell'indagine di rischio per l'ordine di cambiamento.
8. L'utente invia l'indagine e viene visualizzato un messaggio che indica che l'operazione riuscita o meno.

   Se l'invio è riuscito, viene calcolato il livello di rischio e l'ordine di cambiamento viene aggiornato.

Impact Explorer

Impact Explorer è uno strumento avanzato per gestire e controllare i cambiamenti in un'organizzazione. Impact Explorer consente a Gestione Cambiamento di esplorare gli elementi della configurazione associati a un Ordine di cambiamento e di interagire direttamente con un elemento della configurazione associato o con i suoi elementi figlio.

Impact Explorer offre diversi vantaggi:

- Visualizza tutti gli elementi della configurazione associati a un Ordine di cambiamento
- Visualizza tutte le relazioni figlio e peer-to-peer per gli elementi della configurazione associati
- Consente di associare qualsiasi elemento della configurazione all'Ordine di cambiamento
- Visualizza un elenco di elementi figlio di elementi della configurazione correlati successivamente per qualsiasi elemento della configurazione associato
- Consente di avviare CMDB Visualizer per un elemento della configurazione

Ulteriori informazioni:

Avvio di Impact Explorer (a pagina 856)
Esplorazione degli elementi della configurazione associati. (a pagina 856)
Visualizzazione di un elemento della configurazione in Impact Explorer (a pagina 857)
Aggiunta di un elemento della configurazione correlato a un ordine di cambiamento (a pagina 857)
Visualizzazione dell'elenco di elementi della configurazione figlio (a pagina 858)
Avvio di CMDB Visualizer da Impact Explorer (a pagina 858)
Configurazione di Impact Explorer (a pagina 859)

Avvio di Impact Explorer

È possibile accedere a Impact Explorer dalla scheda Elementi della configurazione di qualsiasi ordine di cambiamento.

Per avviare Impact Explorer

1. Aprire una pagina Dettagli ordine di cambiamento.
2. Selezionare la scheda Elementi della di configurazione.
3. Fare clic su Impact Explorer.

   Viene visualizzata la pagina Impact Explorer.

   Nota: se si chiude la pagina Dettagli ordine di cambiamento, viene chiusa anche la pagina Impact Explorer.

Nota: se Impact Explorer viene avviato da più ordini di cambiamento, vengono visualizzate più pagine Impact Explorer.

Esplorazione degli elementi della configurazione associati.

La struttura di Impact Explorer contiene un nodo per ogni elemento della configurazione associato a un ordine di cambiamento. Il simbolo più (+) indica che un elemento della configurazione ha almeno un elemento della configurazione figlio.

Nota: se all'ordine di cambiamento sono associati più di 100 elementi della configurazione, vengono visualizzati solo i primi 100.

Per visualizzare le relazioni per un elemento della configurazione associato, fare clic sul simbolo più (+) per l'elemento della configurazione. Nella struttura vengono visualizzati gli elementi della configurazione correlati. Oltre ai nomi degli elementi della configurazione correlati, la struttura mostra anche i tipi di relazione tra parentesi.

Nota: se all'ordine di cambiamento sono associati più di 100 elementi della configurazione, vengono visualizzati solo i primi 100. Per visualizzare i 100 elementi della configurazione successivi, fare clic su Altro...

Visualizzazione di un elemento della configurazione in Impact Explorer

La struttura di Impact Explorer mostra un nodo per ogni elemento della configurazione associato a un ordine di cambiamento. Il simbolo più (+) indica che un elemento della configurazione ha almeno un elemento della configurazione figlio.

Per visualizzare un elemento della configurazione

1. Fare clic sul nodo di un elemento della configurazione nel riquadro sinistro.

   La pagina Dettagli elemento della configurazione viene visualizzata nel riquadro di destra.

   Nota: è inoltre possibile visualizzare la pagina Dettagli elemento della configurazione nel riquadro di destra facendo clic con il pulsante destro del mouse sull'elemento della configurazione e selezionando Visualizza dal menu di scelta rapida.

2. Fare clic sul nodo dell'ordine di cambiamento nella parte superiore del riquadro sinistro.

   Viene visualizzata la pagina Dettagli ordine di cambiamento.

Nota: se all'ordine di cambiamento sono associati più di 100 elementi della configurazione, vengono visualizzati solo i primi 100. Per visualizzare i 100 elementi della configurazione successivi, fare clic su Altro...

Aggiunta di un elemento della configurazione correlato a un ordine di cambiamento

Mentre si esplorano le relazioni tra gli elementi della configurazione, si potrebbe decidere di associare un elemento della configurazione correlato all'ordine di cambiamento.

Per aggiungere un elemento della configurazione correlato a un ordine di cambiamento

1. Fare clic sulla scheda Elementi della configurazione per un ordine di cambiamento.

   Viene visualizzata la pagina Elenco elementi della configurazione.

2. Fare clic su Impact Explorer.

   La struttura di Impact Explorer mostra gli elementi della configurazione associati.

3. Fare clic su qualsiasi segno più (+) per un nodo di elementi della configurazione associati.

   Vengono visualizzati gli elementi della configurazione correlati al nodo.

4. Fare clic con il pulsante destro del mouse su un elemento della configurazione correlato e selezionare Aggiungi all'ordine di cambiamento dal menu di scelta rapida.

   Il nuovo elemento della configurazione associato compare nella scheda Elementi della configurazione per l'ordine di cambiamento.

Visualizzazione dell'elenco di elementi della configurazione figlio

Per qualsiasi elemento della configurazione è possibile visualizzare righe di elementi della configurazione correlati (detti *elementi figlio*). Oltre alle informazioni di base su ogni elemento della configurazione, l'elenco degli elementi figlio mostrano i livelli di relazione, in cui l'elemento della configurazione fonte è indicato come livello 1. Gli elementi figlio iniziano al livello 2, i loro elementi figlio si trovano al livello 3 e così via. Se un elemento della configurazione viene rilevato più volte fra le relazioni controllate, viene visualizzato solo il livello di relazione più vicino.

Esempio: percorsi multipli di elementi figlio per un elemento della configurazione

Data l'esistenza di più relazioni, una ricerca di elementi figlio trova lo stesso elemento della configurazione correlato al livello 2 e al livello 4. L'elemento della configurazione figlio è visualizzato solo al livello 2.

Per elencare gli elementi figlio di un elemento della configurazione

1. Da una pagina Dettagli ordine di cambiamento, selezionare la scheda Elementi. di configurazione.
2. Fare clic su Impact Explorer per visualizzare gli elementi della configurazione associati.
3. Espandere il nodo di un elemento della configurazione, se necessario.
4. Fare clic con il pulsante destro del mouse su un elemento della configurazione e selezionare Elenca discendenti.

   Viene visualizzato l'Elenco discendenti elemento della configurazione.

Avvio di CMDB Visualizer da Impact Explorer

Impact Explorer consente di avviare CMDB Visualizer da un elemento della configurazione associato o correlato.

Per avviare CMDB Visualizer da Impact Explorer

1. Da una pagina Dettagli ordine di cambiamento, fare clic su Impact Explorer.

   Viene visualizzata la pagina Impact Explorer.

2. Fare clic con il pulsante destro del mouse su un elemento della configurazione qualsiasi e selezionare Launch Visualizer dal menu di scelta rapida.

   CMDB Visualizer viene avviato con l'elemento della configurazione visualizzato.

Configurazione di Impact Explorer

Un amministratore può configurare Impact Explorer come segue:

- Specificare il numero di elementi della configurazione figlio visualizzati per un elemento della configurazione associato
- Specificare il numero di livelli di relazione visualizzati nell'Elenco discendenti elemento della configurazione
- Escludere la visualizzazione degli elementi della configurazione figlio

Il numero di elementi della configurazione figlio visualizzati può essere configurato aggiungendo un'impostazione NX_IMPACT_EXPLORER_MAX_CHILD_NODES al file di configurazione NX.env. L'impostazione predefinita è 100.

Esempio: impostazione della visualizzazione degli elementi della configurazione figlio

Utilizzando l'impostazione riportata di seguito, Impact Explorer visualizza solo dieci elementi figlio alla volta per un elemento della configurazione associato:

@NX_IMPACT_EXPLORER_MAX_CHILD_NODES=10

La profondità predefinita dell'Elenco discendenti elemento della configurazione è di nove (9) livelli. La profondità può essere configurata aggiungendo un'impostazione NX_IMPACT_EXPLORER_MAX_LEVELS al file di configurazione NX.env.

Esempio: configurazione del numero di livelli degli elementi figlio

Utilizzando l'impostazione seguente, l'Elenco discendenti elemento della configurazione mostra l'elemento della configurazione fonte e solo gli elementi figlio con cui ha una relazione prossima:

@NX_IMPACT_EXPLORER_MAX_LEVELS=2

Utilizzare la seguente opzione di Gestione opzioni per escludere la visualizzazione di un tipo specifico di elementi della configurazione figlio:

IMPACT_EXPLORER_EXCLUDE_HIER=boolean

Se l'opzione IMPACT_EXPLORER_EXCLUDE_HIER è installata e impostata su Sì, gli elementi della configurazione figlio che sono correlati attraverso la scheda Relazioni CMDB di una pagina Dettagli elemento della configurazione non vengono visualizzati nella struttura di Impact Explorer o nell'Elenco discendenti elemento della configurazione.

Nota: vengono invece visualizzati gli elementi della configurazione figlio che sono correlati attraverso CA CMDB.

Capitolo 19: Gestione dei rapporti

Questa sezione contiene i seguenti argomenti:

Report CA Business Intelligence (a pagina 863)
Scenari di reporting (a pagina 863)
Componenti del reporting (a pagina 864)
Diagramma di flusso sul reporting dei dati (a pagina 866)
Visualizzazione dei report Web in InfoView (a pagina 867)
Protezione e autorizzazione (a pagina 868)
Modalità di indirizzamento di un server di CA Business Intelligence esistente a un server CA SDM (a pagina 873)
Modalità di configurazione della protezione delle partizioni dati per il reporting (a pagina 875)
Database replicato per il reporting non in linea (a pagina 878)
Report Role-Based (a pagina 878)
Report basati sul Web (a pagina 887)
Indicatori di prestazioni chiave (a pagina 890)
Report ad hoc (a pagina 902)
Esempio di report ad hoc (a pagina 903)
Report del dashboard (a pagina 909)
Scrivere report di CA Business Intelligence (a pagina 910)

Capitolo 20: Report CA Business Intelligence

CA Business Intelligence è un componente basato sul Web che integra la tecnologia BusinessObjects con CA SDM e molte fonti dati di comuni, come SQL Server, Oracle e ODBC (Open Database Connectivity).

CA Business Intelligence utilizza BusinessObjects Enterprise come sistema di reporting predefinito. I report predefiniti vengono forniti per CA SDM, Gestione della conoscenza e Support Automation.

La funzionalità di reporting di CA Business Intelligence consente di eseguire le seguenti operazioni:

- Personalizzare i report esistenti
- Ricercare i dati del report Objects per visualizzare i dati sotto ai grafici e ai gruppi di riepilogo
- Esportare le istanze dei report in formati di output diversi
- Creare report ad hoc
- Pubblicare nuovi report e distribuire a utenti autorizzati
- Pianificare l'esecuzione di report a un orario specifico
- Usare il reporting dashboard per controllare le operazioni giornaliere di tutti i tipi di ticket CA SDM.

Nota: al reporting è possibile accedere solo attraverso la funzione di protezione delle partizioni dati di CA SDM.

Scenari di reporting

CA Business Intelligence integrato con BusinessObjects Enterprise supporta i seguenti scenari di report:

- **Segnalazione basata su ruoli**—Nella scheda Report di CA SDM gli utenti autorizzati possono visualizzare i report definiti per il proprio ruolo, quindi fare clic sul pulsante InfoView per gestire i report personali in BusinessObjects InfoView. CA SDM utilizza l'interfaccia InfoView per raccogliere, organizzare e presentare le informazioni nei formati dei report. In InfoView, i report predefiniti vengono raggruppati in cartelle pubbliche.

- **Report basati sul Web**—I report basati sul Web sono report predefiniti in CA SDM, Gestione della conoscenza, CMDB e Support Automation. Sono sviluppati con Web Intelligence o Crystal Reports. È possibile accedere ai report in InfoView e utilizzarli come modelli per definire report specifici in base al sito.
- **Segnalazione ad hoc**—I report ad hoc vengono creati e gestiti da InfoView utilizzando un'interfaccia Web Intelligence basata su plugin. È possibile memorizzare e gestire report in un'area di lavoro personale (My Folders). Il reporting ad hoc è destinato a utenti che desiderano creare report di base senza scrivere query.
- **Report dashboard**—I rapporti dashboard consentono di monitorare le operazioni giornaliere per tutti i tipi di ticket CA SDM (richiesta/incidente/problema, ordine di cambiamento o questione) in InfoView. Ciascun report contiene informazioni analitiche sulle migliori prestazioni su ticket attivi, in modo da poterne seguire l'andamento. È possibile lavorare con report di dashboard predefiniti individuali o utilizzare la dashboard aziendale per vedere tutte le operazioni CA SDM quotidiane in un'unica visualizzazione.

Componenti del reporting

BusinessObjects Enterprise e i relativi strumenti associati, assieme a BusinessObjects Crystal Reports XI, rappresentano la spina dorsale dell'architettura BI CA.

Sebbene i Crystal Reports siano forniti come componente primario di CA Business Intelligence, lo strumento di creazione e manutenzione dei report, Crystal Reports XI, non è fornito come parte di CA Business Intelligence. Crystal Reports XI è un prodotto con licenza separata che può essere acquistato da BusinessObjects Enterprise e utilizzato assieme a CA Business Intelligence.

Nota: i report predefiniti di Microsoft Access non vengono più sviluppati o forniti con CA SDM.

È possibile utilizzare i seguenti componenti per amministrare, monitorare e configurare l'ambiente di report CA Business Intelligence:

- **Database CA SDM / Domsrvr / Driver ODBC—**I dati dei report vengono memorizzati in un database CA SDM SQL Server o Oracle. Le applicazioni di reporting di BusinessObjects (Crystal Reports e Web Intelligence) accedono al database utilizzando un driver ODBC che li collega direttamente al motore oggetti di CA SDM (domsrvr). Tutta la sicurezza CA SDM, inclusa la partizione dati e le restrizioni di tenancy, viene applicata automaticamente ai report ma non al proprio ambiente di report. È possibile configurare l'ambiente di reporting in modo che utilizzi le partizioni dati esistenti in CA SDM.

  Nota: per informazioni su come stabilire la protezione delle partizioni dati per l'ambiente di reporting, vedere Modalità di configurazione della protezione delle partizioni dati per il reporting (a pagina 868).

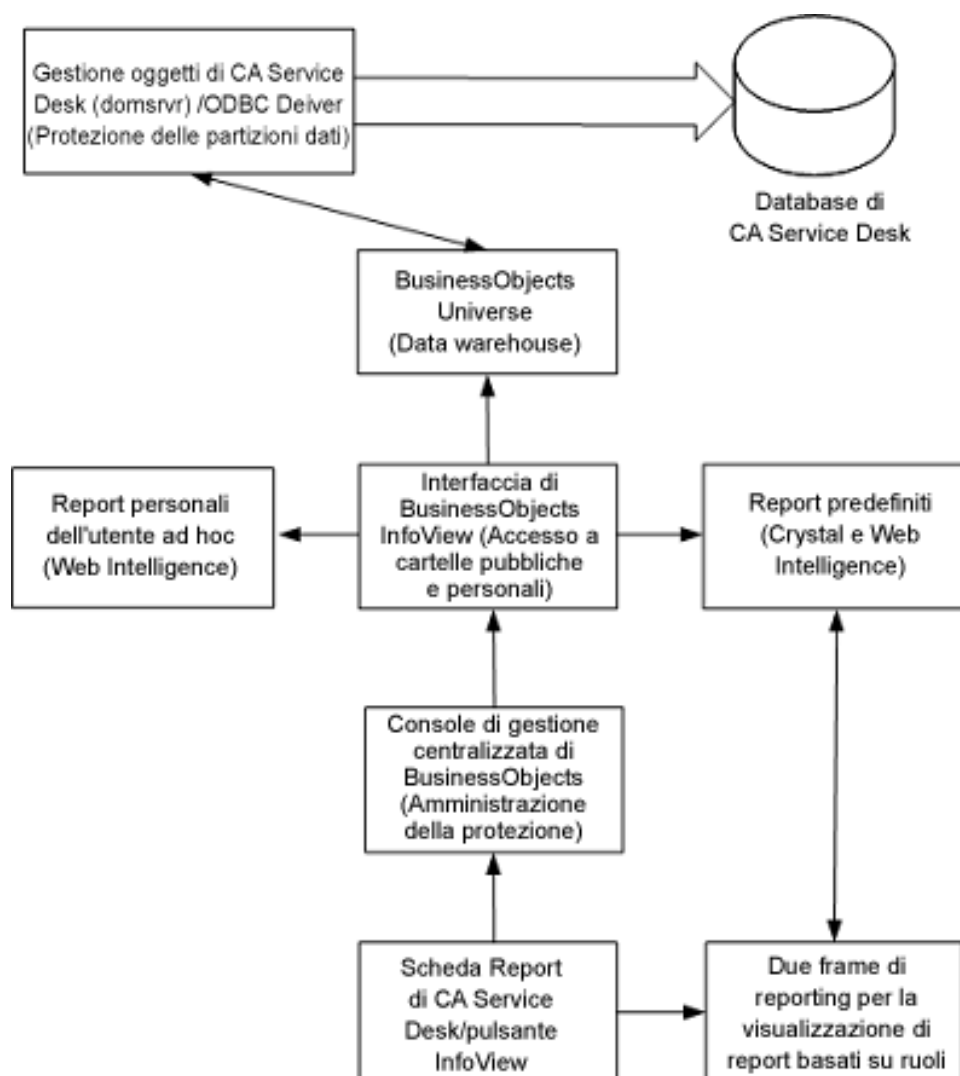
- **Central Management Server (CMS)**—È il repository centrale che memorizza tutti gli oggetti utilizzati in ciascun processo di reporting.
- **Central Management Console—**È un componente amministrativo che fornisce accesso a tutte le funzioni di amministrazione di BusinessObjects. Utilizzando il CMC, è possibile distribuire report e assegnare accesso utente e autorizzazioni di cartella per InfoView. Le opzioni di autenticazione, ruolo e autorizzazione utenti devono essere definite per l'ambiente di reporting utilizzando il CMC.

  Nota: le opzioni di autenticazione, ruolo e autorizzazione utenti devono essere definite per l'ambiente di report prima di utilizzare CA Business Intelligence. Per maggiori informazioni sulla definizione di sicurezza, vedere Protezione e autorizzazione (a pagina 868).
- **Universo BusinessObjects—**Descrive le classi (tabelle) e gli oggetti (colonne) utilizzate nei report. L'universo CA SDM viene installato e configurato durante l'installazione. Al completamento dell'installazione, il collegamento dell'universo viene assegnato a diversi gruppi e utenti in CA SDM.
- **Progettazione—**È un componente di BusinessObjects che consente di modificare l'universo CA SDM, che è un meta layer tra lo schema CA SDM e gli strumenti di reporting di BusinessObjects. La procedura guidata di importazione/esportazione facilita la compilazione o l'estrazione dell'oggetto all'interno del CMS.
- **Report predefiniti**—Sono report CA SDM e Gestione della conoscenza basati sul Web e sviluppati con Web Intelligence o Crystal Reports. I report possono essere utilizzati come modelli per definire report specifici in base ai siti.
- **InfoView—**È un'interfaccia Web che consente agli utenti autorizzati CA SDM di interagire con i report predefiniti basati sul Web, visualizzando, eseguendo e pianificando i tipi di report tra cui Web Intelligence e Crystal Reports. I report sono contenuti in cartelle nella sezione pubblica di InfoView.
- **Report ad hoc—**I report ad hoc consentono di creare e amministrare i report utilizzando un'interfaccia basata su plug-in di Web Intelligence. Questo strumento è pensato per utenti che desiderano creare report di base senza scrivere query.

  Nota: per esempi sull'uso di report ad hoc, vedere Report ad hoc (a pagina 902).
- **Report dashboard**—I rapporti dashboard consentono di monitorare le operazioni giornaliere per tutti i tipi di ticket CA SDM (richiesta/incidente/problema, ordine di cambiamento o questione) in BusinessObjects InfoView. Ciascun report contiene informazioni analitiche sulle migliori prestazioni su ticket attivi, in modo da poterne seguire l'andamento.
- **Scheda Report di CA SDM—**Dalla scheda Report gli utenti autorizzati possono visualizzare i report basati su ruoli di CA SDM, quindi fare clic sul pulsante InfoView in questa scheda per gestire i report personali in InfoView.

  Nota: per informazioni su come gestire report basati sul ruolo e visualizzare nuovi report sulla scheda Report, vedere Report basati sul Web (a pagina 887).

Diagramma di flusso sul reporting dei dati

Il diagramma seguente illustra il flusso dei dati del componente e l'esecuzione per CA Business Intelligence integrato con BusinessObjects Enterprise:

Visualizzazione dei report Web in InfoView

CA SDM utilizza l'interfaccia BusinessObjects InfoView per raccogliere, organizzare e presentare le informazioni nei formati dei report.

Importante Durante la generazione di report, è *necessario* aggiornare i campi Data. Gli altri campi sono facoltativi.

Procedere come descritto di seguito:

1. Dalla scheda Report in CA SDM, fare clic sul pulsante InfoView.

   Viene visualizzata la pagina iniziale InfoView.

2. Dal riquadro Intestazione, selezionare Elenco Documenti.

   L'elenco dei documenti contiene i report CA SDM, gli strumenti di amministrazione, gli esempi etc. contenuti in cartelle pubbliche. Quando viene selezionata una cartella, il contenuto corrispondente viene visualizzato nel riquadro Dettagli. L'accesso alle cartelle dell'Elenco Documenti dipende dai diritti che vengono concessi all'utente dall'amministratore.

   Ad esempio, per visualizzare i report di CMDB, è necessario accedere a CA Service Desk/CMDB. Il riquadro Dettagli conterrà un elenco di report.

3. Fare doppio clic su un report.

   Viene visualizzato il modulo Report. Il modulo contiene i campi corrispondenti immessi dall'utente e consente di generare il report selezionato.

4. Immettere le informazioni necessarie per la generazione del report selezionato.

   Esempio: se viene aperto il report sugli elementi della configurazione aggiunti durante il periodo, sarà necessario specificare il periodo per cui si desidera visualizzare gli elementi della configurazione aggiunti, i nomi dei titolari dell'elemento della configurazione, ecc.

   Importante Se si utilizza il database Oracle e si desidera generare il report sugli impatti di tutti i Cambiamenti, il report sulle relazioni degli elementi della configurazione ed il report Analisi causa principale, selezionare Oracle (i report funzioneranno soltanto per Oracle) dalla cartella CMDB ed accedere ai report. Se i report vengono generati dalla cartella SQL Server, verrà visualizzato un messaggio di errore e i report non verranno generati. Se si utilizza il database SQL e si desidera generare il report sugli impatti di tutti i Cambiamenti, il report sulle relazioni degli elementi della configurazione ed il report Analisi causa principale, selezionare il server SQL (i report funzioneranno soltanto per il server SQL) dalla cartella CMDB ed accedere ai report.

   Nota: per poter generare il report è necessario completare tutti i campi.

5. Fare clic su OK.

   Viene visualizzato il report.

Nota: BusinessObjects InfoView include una Guida per l'utente che descrive l'utilizzo di BusinessObjects InfoView. Per accedere alla Guida dell'utente, fare clic sull'icona della guida in linea di InfoView.

Protezione e autorizzazione

La configurazione di sicurezza predefinita per BusinessObjects Enterprise viene eseguita attraverso la configurazione di CA Business Intelligence. La configurazione determina le policy di sicurezza di cartelle, universi, collegamenti di universi e strumenti. Fornisce inoltre metodi per l'aggiunta di utenti e la relativa mappatura a gruppi, oltre all'impostazione di alcune opzioni di preferenza.

In particolare, la configurazione di reporting di CA Business Intelligence coinvolge i punti seguenti:

- Impostazione della sicurezza
- Distribuzione dei report
- Distribuzione degli universi
- Configurazione impostazioni di Web Intelligence

Al completamento dell'installazione, il collegamento dell'universo viene assegnato a diversi gruppi e utenti in CA SDM.

L'amministratore può accedere al CMC BusinessObjects e modificare le impostazioni predefinite in qualsiasi momento. Agli utenti viene autorizzato l'accesso alle cartelle InfoView in base al gruppo CA Business Intelligence a cui appartengono.

Gruppi e utenti

I gruppi elencati nella seguente tabella verranno aggiunti al Central Management Server (CMS) durante la configurazione di CA Business Intelligence. Sono correlati ai ruoli di CA SDM con gli stessi nomi. Durante la fase di configurazione, era disponibile una casella di controllo opzionale per indicare se aggiungere utenti di prova al CMS. Se è stata selezionata, la configurazione predefinita di CMS include un utente di esempio per ciascun gruppo. Nella CMC è possibile utilizzare gli utenti di esempio come modelli per stabilire le autorizzazioni utente e le opzioni di autenticazione per l'ambiente di reporting.

Nome gruppo	Nome utente
Gestione Cambiamento	Utente gestione Cambiamento
Gestione servizio clienti	Utente gestione servizio clienti
Gestione della conoscenza	Utente Gestione della conoscenza

Nome gruppo	Nome utente
Analista della conoscenza	Utente analista della conoscenza
Gestione Service Desk	Utente gestione Service Desk
Gestione Incidente	Utente Gestione incidente
Gestione problemi	Utente Gestione problemi

Partizioni di dati CA SDM in Infoview

Considerare le informazioni seguenti sulle relazioni tra partizioni di dati CA SDM e InfoView:

- L'analista esegue l'accesso a CA Business Intelligence mediante la scheda Report di CA SDM o InfoView con il tipo di accesso associato al ruolo di reporting predefinito.
- Le credenziali di accesso di CA SDM *devono* corrispondere a quelle di InfoView. L'amministratore imposta un metodo di autenticazione come ad esempio secLDAP o secEnterprise. CA SDM esegue l'accesso a CA Business Intelligence, il quale a sua volta esegue l'accesso a CA SDM mediante ODBC.
- La connessione dell'analista di CA Business Intelligence è associata alla connessione CA SDM. CA Business Intelligence utilizza la connessione CA SDM ed il ruolo di reporting associato al tipo di accesso della connessione. Se l'analista non dispone di un accesso a CA SDM associato, CA Business Intelligence utilizzerà le impostazioni predefinite del sistema. Il valore di sistema predefinito viene definito nei parametri ODBC in Universe Designer ed il ruolo di reporting del tipo di accesso.
- Per impedire a un utente di visualizzare un report, l'amministratore può disattivare l'accesso al report o alla cartelle contenente il report.

Universo e collegamenti dell'universo

La configurazione predefinita include anche la policy protezione per accedere all'universo CA SDM e le connessioni degli universi. Per consentire un accesso completo, tutti i gruppi predefiniti dispongono di accesso a controllo completo.

Nome gruppo	Livello di accesso
Gestione Cambiamento	Controllo completo
Gestione servizio clienti	Controllo completo
Analista della conoscenza	Controllo completo
Gestione della conoscenza	Controllo completo
Gestione Service Desk	Controllo completo

Nome gruppo	Livello di accesso
Gestione Incidente	Controllo completo
Gestione problemi	Controllo completo

Cartelle di report

La configurazione predefinita viene fornita con una serie di cartelle contenenti report predefiniti per CA SDM e Gestione della conoscenza. Ciascun gruppo CA SDM viene configurato per l'accesso a una serie secondaria di queste cartelle.

Nome cartella	Nome gruppo	Livello di accesso
Aggrega	■ Gestione Cambiamento ■ Gestione servizio clienti ■ Gestione della conoscenza ■ Analista della conoscenza ■ Gestione Service Desk ■ Gestione Incidente ■ Gestione problemi	■ Visualizza ■ Visualizza ■ Nessun accesso ■ Nessun accesso ■ Controllo completo ■ Visualizza ■ Visualizza
Asset	■ Gestione Cambiamento ■ Gestione servizio clienti ■ Gestione della conoscenza ■ Analista della conoscenza ■ Gestione Service Desk ■ Gestione Incidente ■ Gestione problemi	■ Visualizzazione su richiesta ■ Visualizza ■ Nessun accesso ■ Nessun accesso ■ Controllo completo ■ Visualizza ■ Visualizza
Ordine di cambiamento (include tutte le cartelle secondarie)	■ Gestione Cambiamento ■ Gestione servizio clienti ■ Gestione della conoscenza ■ Analista della conoscenza ■ Gestione Service Desk ■ Gestione Incidente ■ Gestione problemi	■ Controllo completo ■ Nessun accesso ■ Nessun accesso ■ Nessun accesso ■ Visualizza ■ Visualizza ■ Visualizza

Nome cartella	Nome gruppo	Livello di accesso
Issue (include tutte le cartelle secondarie)	■ Gestione Cambiamento ■ Gestione servizio clienti ■ Gestione della conoscenza ■ Analista della conoscenza ■ Gestione Service Desk ■ Gestione Incidente ■ Gestione problemi	■ Nessun accesso ■ Controllo completo ■ Nessun accesso ■ Nessun accesso ■ Nessun accesso ■ Nessun accesso ■ Nessun accesso
Richiesta (include tutte le cartelle secondarie)	■ Gestione Cambiamento ■ Gestione servizio clienti ■ Gestione della conoscenza ■ Analista della conoscenza ■ Gestione Service Desk ■ Gestione Incidente ■ Gestione problemi	■ Nessun accesso ■ Nessun accesso ■ Nessun accesso ■ Nessun accesso ■ Controllo completo ■ Visualizza ■ Nessun accesso
Gestione della conoscenza	■ Gestione Cambiamento ■ Gestione servizio clienti ■ Gestione della conoscenza ■ Analista della conoscenza ■ Gestione Service Desk ■ Gestione Incidente ■ Gestione problemi	■ Nessun accesso ■ Visualizza ■ Controllo completo ■ Visualizza ■ Pianifica ■ Visualizza ■ Visualizza
Indagine	■ Gestione Cambiamento ■ Gestione servizio clienti ■ Gestione della conoscenza ■ Analista della conoscenza ■ Gestione Service Desk ■ Gestione Incidente ■ Gestione problemi	■ Nessun accesso ■ Nessun accesso ■ Visualizza ■ Nessun accesso ■ Controllo completo ■ Visualizza ■ Visualizza

Nome cartella	Nome gruppo	Livello di accesso
Incident and Problem Management	■ Gestione Cambiamento ■ Gestione servizio clienti ■ Gestione della conoscenza ■ Analista della conoscenza ■ Gestione Service Desk ■ Gestione Incidente ■ Gestione problemi	■ Nessun accesso ■ Nessun accesso ■ Visualizza ■ Nessun accesso ■ Pianifica ■ Controllo completo ■ Controllo completo

Livelli di accesso

La configurazione predefinita include i seguenti livelli di accesso per gruppi e utenti:

Nessun accesso

Imposta tutte le autorizzazioni su Non specificato.

Visualizza

Consente all'utente di vedere la cartella, il report o l'universo. Se il report contiene dati, l'utente potrà aprirlo e interagire con esso. Se il report non contiene dati, l'utente non potrà aggiornare il report. Per impostazione predefinita, l'utente può modificare il report e salvarlo in una cartella personale, aggiornandolo successivamente. È possibile impedire in modo esplicito agli utenti di copiare documenti aziendali in cartelle personali impostando un diritto individuale che impedisca la copia di oggetti in un'altra cartella.

Pianifica

Consente a un utente di pianificare un report ma non di aggiornarlo in tempo reale.

Visualizzazione su richiesta

Consente a un utente di aggiornare un report in tempo reale. Se il report è un documento Web Intelligence, l'utente deve disporre dell'accesso di tipo Visualizzazione su richiesta all'universo e alla connessione dell'universo per eseguire l'aggiornamento.

Controllo completo

Consente a un utente di creare nuovi report all'interno di una cartella, oltre a modificare report esistenti o eliminare voci.

Avanzate

Quando i livelli di accesso precedenti non soddisfano le proprie esigenze, viene garantito un accesso più dettagliato scegliendo l'opzione avanzata.

Se il livello di accesso di un utente o di un gruppo è impostato su Avanzate, si dispone di un controllo più dettagliato dei diritti rispetto ai tipi di accesso Visualizza, Pianifica, Visualizzazione su richiesta o Controllo completo.

Le cartelle BusinessObjects utilizzano una sicurezza ereditata. Per le cartelle di livello inferiore si riceve la stessa autorità della cartella di livello superiore assegnata all'utente o al relativo gruppo, a meno che non vengano applicate restrizioni per ignorarla a livelli inferiori. Autorizzazioni predefinite vengono fornite a livello di cartella e a livello di gruppo. Gli utenti erediteranno i diritti del proprio gruppo per tutti gli oggetti nella cartella e nelle relative cartelle secondarie.

CA Business Intelligence viene installato con due gruppi: Amministratori e Tutti. Al gruppo Tutti viene assegnato un Livello di accesso di Pianificazione che consente la pianificazione e la visualizzazione di tutti gli oggetti report.

Ulteriori informazioni:

Cartelle di report (a pagina 870)

Modalità di indirizzamento di un server di CA Business Intelligence esistente a un server CA SDM

Se è presente un server CA Business Intelligence, è possibile indirizzarlo a un server CA SDM nel modo seguente:

1. Creazione di una nuova fonte dati ODBC (a pagina 873).
2. Configurazione dell'universo. (a pagina 874)
3. Esportazione dell'universo. (a pagina 875)
4. Avvio di InfoView per verificare la connessione.

Creazione di una fonte dati ODBC.

È possibile creare una fonte dati ODBC sul server di CA Business Intelligence tramite Amministratore origine dati ODBC.

Per creare una fonte dati ODBC

1. Selezionare Start, Programmi, Strumenti di amministrazione, Fonte dati (ODBC).

   Viene visualizzata la pagina Amministratore origine dati ODBC.

2. Fare clic sulla scheda DSN di sistema, quindi su Aggiungi.

   Viene visualizzata la pagina Crea nuova fonte dati.

3. Selezionare DataDirect OpenAccess e fare clic su Termina.

   Viene visualizzata la pagina di impostazione ODBC di DataDirect OpenAccess.

4. Specificare casd_*nomeserver* nel campo Nome ODBC.

5. Fare clic su Avanzate.

   Viene visualizzata la pagina Avanzate.

6. Fare clic su Aggiungi.

   Viene visualizzata la pagina di impostazione database di Open Access.

7. Inserire i dati nei seguenti campi:

   - **Nome**. Specificare casd_*nomeserver*.
   - **Indirizzo IP**. Specificare il *nomeserver* o l'indirizzo IP.

     Nota: effettuare il ping del *nomeserver* per determinare l'indirizzo IP da utilizzare al posto del *nomeserver*.
   - **Porta**. Specificare 1706.
   - **Tipo**. (Facoltativo) Specificare il database usato nel server. Questo campo viene utilizzato solo come informazione di riferimento.

8. Fare clic su OK.

9. Selezionare casd_*nomeserver* dall'elenco a discesa Database.

10. Fare clic su OK.

    La fonte dati ODBC è stata creata.

Configurazione dell'universo

Dopo aver creato una fonte dati ODBC, occorre configurare l'universo stabilendo una connessione tra <USDK> e CA Business Intelligence.

Per configurare l'universo

1. Avviare Progettazione e accedere come amministratore.

2. Fare clic su File, Importa.

   Verrà visualizzata la pagina Import Universe (Importazione universo).

3. Sfogliare e selezionare l'universo CA SDM, quindi fare clic su OK.

   Verrà visualizzato il messaggio di importazione dell'universo andata a buon fine.

4. Fare clic su File, quindi su Parametri.

   Verrà visualizzata la pagina Universe Parameters (Parametri universo).

5. Fare clic su Modifica.

   Viene visualizzata la pagina di modifica del collegamento CA SDM.

6. Specificare il nome utente e la password dell'utente privilegiato CA SDM, ad esempio ServiceDesk.

7. Selezionare casd_*nome server* dal nome della fonte dati e fare clic su Avanti.

8. Fare clic su Test connessione per verificare che l'universo CA SDM comunichi con CA Business Intelligence.

9. Fare clic su Avanti, Avanti e quindi su Fine.

   L'universo è ora configurato.

Esportazione dell'universo

Una volta configurato l'universo, è necessario esportarlo da Progettazione.

Per esportare l'universo

1. Fare clic su File, quindi su Esporta.

   Viene visualizzata la finestra di dialogo Esporta universo.

2. Fare clic su Continua.

3. Fare clic su OK.

   L'universo verrà esportato.

Modalità di configurazione della protezione delle partizioni dati per il reporting

L'accesso al reporting CA Business Intelligence è limitato attraverso la funzione di protezione delle partizioni dati di CA SDM. Tutta la sicurezza CA SDM, incluse le restrizioni tenancy e di partizione dati, viene applicata automaticamente ai report.

La sicurezza della partizione dati per il proprio ambiente di reporting specifico non viene applicata durante la fase di configurazione. È possibile configurare l'ambiente di reporting in modo che utilizzi le partizioni dati esistenti in <USDK>.

A questo scopo, vengono utilizzati i seguenti strumenti:

- **BusinessObjects Central Management Console** (CMC)—Consente di amministrare le autorizzazioni e l'autenticazione utente di BusinessObjects Enterprise.
- **BusinessObjects Designer**—Consente di modificare l'universo per CA SDM, Gestione della conoscenza, CMDB e Support Automation, che rappresenta un meta layer tra schema CA SDM e strumenti di reporting.
- **Gestione protezione e ruoli CA SDM**—Consente di impostare la sicurezza delle partizioni dati per determinare a quali dati possono accedere gli utenti.

Aggiungere l'utente privilegiato CA SDM a CMC

Il collegamento dell'universo viene configurato in modo predefinito per l'uso dell'utente privilegiato e della password di Service Desk quando si accede ai dati. Questo utente deve essere aggiunto al CMC come nuovo utente CA Business Intelligence. Vi sono due motivi per l'aggiunta di questo utente. In primo luogo, questo utente sarà necessario se si pianifica di impostare la protezione di partizioni dati per attività di reporting e, in secondo luogo, consentirà di utilizzare l'utente durante la fase iniziale di testing dei report nella scheda Report di CA SDM. La scheda Report richiede un utente definito per CA SDM e CA Business Intelligence.

Utilizzare le istruzioni fornite nella *Guida all'implementazione* per aggiungere gli utenti CA SDM al CMC e configurare l'account utente Privilegiato CA SDM.

Definizione di credenziali del database universo

L'universo deve utilizzare le credenziali di database associate con l'account utente BusinessObjects.

Nota: assicurarsi di accedere a BusinessObjects Designer utilizzando l'account utente con privilegi e non l'account utente amministratore.

Definizione di credenziali del database universo

1. Dal menu Start accedere a Tutti i programmi, BusinessObjects XI, BusinessObjects Enterprise, Designer.
2. Accedere a Designer.

   Viene visualizzata la finestra Designer.
3. Selezionare File, Import.

   Viene visualizzata la finestra di dialogo Import Universe (Importa universo).
4. Selezionare la cartella CA SDM, Gestione della conoscenza, CMDB o Support Automation dall'elenco a discesa.

   Nota: se si utilizza Designer per la prima volta, selezionare Browse, CA Universes.

5. Verificare il percorso della cartella di importazione nella casella Import Folder (Importazione cartella).
6. Fare clic su OK.

   Viene visualizzata la finestra universo.
7. Selezionare File, Parameters.

   Viene visualizzata la finestra di dialogo Universe Parameters.
8. Fare clic su Definition nella scheda Edit.

   Viene visualizzata la finestra di dialogo Login Parameters (Parametri di accesso).
9. Selezionare la casella di controllo Use database credentials associated with Business Objects user account.
10. Fare clic su Next, Test Connection e seguire le istruzioni nelle finestre di dialogo visualizzate per la connessione dell'universo.
11. Per terminare l'operazione, fare clic su OK.
12. Selezionare File, Export.

    Viene visualizzata la finestra di dialogo di esportazione dell'universo.
13. Selezionare l'universo che si desidera utilizzare dall'elenco a discesa Domain (Dominio).
14. Selezionare Everyone dell'elenco Groups.
15. Fare clic su OK per esportare i cambiamenti all'universo.

Definizione delle partizioni dati

In Gestione ruoli e protezione, creare un vincolo partizione dati che limiti l'accesso ai record di database per tutti gli utenti di report assegnati alla partizione dati.

Nota: per informazioni su come definire vincoli partizioni dati, vedere Impostazione delle partizioni dati (a pagina 300).

Database replicato per il reporting non in linea

Per gestire i possibili problemi di prestazioni che potrebbero interessare i componenti di reporting installati con CA SDM, è possibile creare un database replicato in modo da poterlo utilizzare per il reporting non in linea.

Nota: per ulteriori informazioni sulla creazione di un database replicato per il reporting non in linea, consultare la documentazione e gli script di esempio contenuti nella directory NX_ROOT\samples\reporting.

Report Role-Based

In <USDK> i report basati su ruoli sono visualizzati in due frame di reporting nella scheda Report. Ogni frame fornisce visualizzazioni grafiche che consentono agli utenti di eseguire il drill down dei dati dei report per visualizzare tali dati sotto a grafici e gruppi di riepilogo. È possibile gestire i report basati su ruoli e visualizzare nuovi report BusinessObjects nella scheda Report.

Nella pagina Reports List sono contenuti i dettagli di report disponibili per l'utilizzo. Fare clic sull'icona Elenco report che compare nel frame selezionato per visualizzare questa pagina.

Definizione dei report basati su ruoli per un ruolo

È possibile gestire i moduli Web del report visualizzati nella pagina Elenco Report quando un utente a cui è stato assegnato il ruolo specificato accede al sistema.

Per definire un report basato su ruoli per un ruolo:

1. Selezionare Gestione ruoli e protezione, Gestione ruoli, Elenco ruoli nella scheda Amministrazione.

   Viene visualizzata la pagina Elenco ruoli. Sono disponibili i seguenti ruoli predefiniti per il reporting:

   - Gestione Cambiamento
   - Gestione servizio clienti
   - Gestione della conoscenza
   - Analista della conoscenza

- Gestione Service Desk
- Gestione incidente
- Gestione problemi

2. Selezionare *uno* dei ruoli di reporting dall'elenco.

   Viene visualizzata la pagina Dettagli ruolo modulo. Questa pagina include le seguenti schede:

   Autorizzazione

   Consente di definire il livello di autorizzazione assegnato al ruolo.

   Accesso alle funzioni

   Definisce l'accesso al ruolo a ciascuna area funzionale di CA SDM.

   Interfaccia Web

   Consente di personalizzare l'interfaccia Web per il ruolo mediante la definizione di pagine Web e contenuti di guida in linea ai quali gli utenti possono accedere.

   Gestione della conoscenza

   Specifica i privilegi Gestione della conoscenza assegnati al ruolo.

   Visibilità documento SC

   Specifica gli stati dei documenti che il ruolo è autorizzato a visualizzare; ad esempio Bozza, Ritirato e Pubblicato.

   Schede

   Consente di definire le schede che vengono visualizzate quando un utente assegnato al ruolo accede a CA SDM.

   Moduli Web report

   Consente di definire i moduli Web report disponibili per il ruolo.

   Risorse di accesso rapido

   Consente di specificare quali tipi di record compariranno nell'elenco a discesa Vai per il ruolo. Nella pagina Dettagli ruolo selezionare la scheda Moduli Web di report.

3. Fare clic sulla scheda Moduli Web di report.

   Viene visualizzata la pagina Elenco moduli Web di report. Questa pagina visualizza i dettagli dei report disponibili per l'uso.

4. Fare clic su Update Web Forms.

   Viene visualizzata la pagina Ricerca modulo Web.

5. Immettere i criteri di ricerca per visualizzare i moduli Web desiderati e fare clic su Cerca.

   Viene visualizzata la pagina Web Forms Assigned Update, che elenca i moduli corrispondenti ai criteri di ricerca.

6. Dall'elenco di sinistra, scegliere i moduli Web da visualizzare per questo ruolo. Per selezionare più elementi, tenere premuto il tasto Ctrl mentre si fa clic con il pulsante sinistro del mouse.

7. Una volta selezionati tutti i moduli desiderati, fare clic su Seleziona.

   I moduli selezionati passeranno all'elenco Web Forms Assigned di destra.

8. Fare clic su OK.

   Viene visualizzata la pagina Dettagli ruolo, dove i moduli Web selezionati sono elencati nella scheda Moduli Web report.

Visualizzazione dei nuovi report nella scheda Report

Se un report viene approvato per essere utilizzato in CA SDM, viene spostato nella sezione pubblica di InfoView, diventando così disponibile per gli utenti autorizzati. Per aggiungere un report a CA SDM, l'amministratore deve effettuare anche una serie di ulteriori operazioni.

È possibile visualizzare i nuovi report creati in CA Business Intelligence nella scheda Report di CA SDM. A questo scopo, vengono utilizzati i seguenti strumenti:

- Screen Painter Web
- Gestione ruoli

Prima di iniziare, effettuare le seguenti operazioni:

- Installare e configurare CA Business Intelligence in modo che possa funzionare con CA SDM.

  Nota: per informazioni sull'installazione, vedere la *Guida all'implementazione* e la *Guida all'installazione di CA Business Intelligence*.

- Aver stabilito le autorizzazioni, i ruoli e le opzioni di autenticazione (a pagina 868) per gli utenti nell'ambiente di reporting.

Fase 1: Creazione di due record di moduli Web per richiamare i nuovi report

Per impostazione predefinita, la scheda Report contiene due frame di reporting che consentono agli utenti autorizzati di visualizzare i nuovi report. In questa fase è necessario creare due record di moduli Web e definire gli URL che puntano ai nuovi report.

Per creare due record di moduli Web per richiamare i report:

1. Selezionare Gestione ruoli e protezione, Gestione ruoli, Moduli Web nella scheda Amministrazione.

   Viene visualizzata la pagina Elenco moduli Web.

2. Fare clic su Crea nuovo.

   Viene visualizzata la pagina Crea nuovo modulo Web.

3. Compilare i campi come segue:

   Nome modulo Web

   Consente di specificare il nome che identifica il modulo Web. È un campo obbligatorio.

   Esempio: report Elenco Asset

   Stato record

   Indica che il record è attivo.

   Codice

   Consente di specificarere il valore univoco del codice che identifica il modulo Web nel sistema. Il codice, una volta definito, non può essere modificato.

   Esempio: asset_list

   Nota: prendere nota del valore inserito nel campo Codice.

   Tipo

   Selezionare Report.

   Descrizione

   (Opzionale) Immettere una breve descrizione del modulo Web.

   Risorsa

   Consente di specificare l'URL che richiama il nuovo report.

   Esempio: aprire il modulo Web Elenco Asset dalla pagina Elenco Moduli Web in Gestione ruoli e specificare l'URL che compare in questo modulo.

   ```
   $BOServerURL?sPath=[Home],[Public+Folders],[CA+Reports],[CA+Service+Desk]
   ,[Asset]&sDocName=Asset+List&sViewer=html
   ```

4. Fare clic su Salva.

   La definizione del modulo Web viene salvata e compare la pagina Dettagli modulo Web.

5. Ripetere le fasi 1-3 per creare il secondo record del modulo Web che richiama l'URL del secondo report. Prendere nota del valore immesso nel campo Codice.

Passaggio 2: creazione di una pagina multiframe e assegnazione dei nuovi report

In Web Screen Painter, creare una pagina Web multiframe con due frame verticali, chiamata Set di frame. Quindi, assegnare i record del modulo Web creati nella fase 1 al Set di frame.

Nota: è possibile usare qualsiasi numero di frame per creare la pagina. Tuttavia, è importante ricordare che l'aggiunta di frame supplementari limiterà la visibilità nella scheda Report.

Per creare una pagina multiframe e assegnarla ai report:

1. In Web Screen Painter, selezionare File, Nuovo.

   Viene visualizzata la finestra di dialogo Nuovo modulo.

2. Compilare i campi dell'interfaccia e del gruppo di moduli in modo appropriato.

3. Selezionare un modello multiframe dall'elenco Nome file.

4. Fare clic su Nuovo.

   Viene visualizzata la finestra multiframe.htmpl.

5. Selezionare Controlli e Inserisci Set di frame.

   Viene visualizzata la finestra di dialogo Inserisci Set di frame.

6. Accettare le impostazioni predefinite e fare clic su OK.

   Vengono visualizzati due frame verticali nel Set di frame.

7. Fare clic con il pulsante destro del mouse sul frame verticale e selezionare Proprietà dal menu di scelta rapida.

   Viene visualizzata la finestra di dialogo Proprietà - Set di frame..

8. Selezionare il campo vuoto vicino all'attributo web_form_name, quindi fare clic sul pulsante (...).

   Viene visualizzata la finestra di dialogo Inserisci il nome del modulo Web.

9. Specificare il valore del codice del primo report.

   Esempio: asset_list

10. Appena viene trovato il nome del modulo Web del report fare clic su Esegui validazione.

11. Fare clic con il pulsante destro del mouse sul frame verticale destro, specificare il valore del codice del secondo report, quindi eseguire la validazione del report.

12. Salvare la pagina multiframe.htmpl. Prendere nota del nome del file.

    Esempio: report_mframe.htmpl

13. Scegliere File, Pubblica.

    La pubblicazione rende il modulo disponibile a tutti gli utenti CA SDM. Per il ruolo dell'analista il file è disponibile nella seguente ubicazione: Program Files/CA/Service Desk/Site/mods/www/htmpl/web/analyst/report_mframe.htmpl.

    Nota: quando si cercano moduli Web multiframe in CA SDM, selezionare Gestione ruoli e protezione, Gestione ruoli, Moduli Web nella scheda Amministrazione. La colonna Codice indica web_form_name nella scheda Proprietà per un modulo multiframe in Web Screen Painter.

Fase 3: Creazione di una pagina di inizio per la scheda Report

In Gestione ruoli, creare una pagina di inizio per richiamare la pagina Web multiframe creata nella fase 2.

Per creare una pagina di inizio per la scheda Report:

1. Selezionare Gestione ruoli e protezione, Gestione ruoli, Moduli Web nella scheda Amministrazione.

   Viene visualizzata la pagina Elenco moduli Web.

2. Fare clic su Crea nuovo.

   Viene visualizzata la pagina Crea nuovo modulo Web.

3. Inserire i dati nei seguenti campi:

   Nome modulo Web

   Consente di specificare il nome che identifica il modulo Web. Questo campo è obbligatorio.

   Esempio: pagina di inizio

   Stato record

   Consente di specificare se il record attivo o inattivo.

   Codice

   Consente di specificare il valore univoco del codice che identifica il modulo Web nel sistema. Il codice, una volta definito, non può essere modificato.

   Esempio: start_page

Tipo

Specifica HTMPL.

Descrizione

(Opzionale) Consente di specificare una breve descrizione del modulo Web.

Risorsa

Consente di specificare l'URL che richiama il nuovo report.

Esempio: selezionare il record Multiframe report di Amministrazione nella pagina Elenco Moduli Web. Consente di specificare l'URL che compare in questo modulo. Alla fine di questo percorso, specificare la nuova pagina multiframe (report_mframe.htmpl).

```
$cgi?SID=$SESSION.SID+FID=123+OP=DISPLAY_FORM+HTMPL=report_mframe.htmpl
```

Fare clic su Salva.

Viene visualizzata la nuova pagina di inizio nella pagina Elenco Moduli Web.

Fase 4: Creazione di un record per la scheda Report e assegnazione del record alla pagina di inizio

In Gestione ruoli, creare una nuova scheda Report e specificare la pagina di inizio creata nella fase 3.

Per creare una scheda e assegnarla alla pagina che richiama i report:

1. Selezionare Gestione ruoli e protezione, Gestione ruoli, Schede nella scheda Amministrazione.

   Viene visualizzata la pagina Elenco schede.

2. Fare clic su Crea nuovo.

   Viene visualizzata la pagina Crea nuova scheda.

3. Inserire i dati nei seguenti campi:

   Nome scheda

   Consente di specificare il nome che identifica la scheda nell'interfaccia amministrativa. Ad esempio, il nome della scheda compare alla pagina Elenco Schede.

   Esempio: scheda Report

   Codice

   Consente di specificare il codice che identifica la scheda nel sistema. Il codice, una volta definito, non può essere modificato.

   Esempio: reports_tab

Stato record

Indica che il record è attivo.

Nome visualizzato

Consente di specificare il nome visualizzato nella rappresentazione grafica della scheda nell'interfaccia utente.

Esempio: scheda Report

Pagina di avvio

Consente di specificare il modulo Web iniziale che viene visualizzato nella finestra principale se un utente seleziona questa scheda.

Esempio: pagina di inizio

4. Fare clic su Salva.

   Il modulo viene visualizzato nella pagina Elenco Moduli Web.

Fase 5: Assegnazione del record della scheda a un record Ruolo

In Gestione ruoli, assegnare la scheda Report al ruolo desiderato elencato nella pagina Dettagli ruolo. Quando un utente con questo ruolo accede al sistema, vede la nuova scheda Report nell'interfaccia Web.

Per assegnare il record della scheda a un record Ruolo:

1. Selezionare Gestione ruoli e protezione, Gestione ruoli, Elenco ruoli nella scheda Amministrazione.

   Viene visualizzata la pagina Elenco ruoli.

2. Selezionare il ruolo desiderato dall'elenco Ruolo.

   Viene visualizzata la pagina Dettagli ruolo.

3. In fondo alla pagina, selezionare Schede, quindi Aggiorna schede.

   La nuova condizione viene visualizzata in Elenco Schede.

Creazione di una pagina di inizio per il pulsante InfoView

È possibile scegliere di includere il pulsante InfoView che apre BusinessObjects in una nuova finestra nella scheda Report. Questa operazione può essere effettuata tramite l'opzione Pagina di avvio visualizzata nel record della scheda Report.

Per creare una pagina di inizio per il pulsante InfoView:

1. Selezionare Gestione ruoli e protezione, Gestione ruoli, Moduli Web nella scheda Amministrazione.

   Viene visualizzata la pagina Elenco moduli Web.

2. Fare clic su Crea nuovo.

   Viene visualizzata la pagina Crea nuovo modulo Web.

3. Inserire i dati nei seguenti campi:

   Nome modulo Web

   (Obbligatorio) Specifica il nome che identifica il modulo Web.

   Esempio: pagina InfoView

   Stato record

   Consente di specificare se il record attivo o inattivo.

   Codice

   Specifica il codice che identifica il modulo Web nel sistema.

   Esempio: info_view_page

   Tipo

   Specifica HTMPL.

   Descrizione

   (Opzionale) Descrive il modulo Web.

   Risorsa

   Specifica l'URL che richiama i frame di reporting.

   Esempio: selezionare il record InfoView Amministratore nella pagina Elenco Moduli Web. Consente di specificare l'URL che compare in questo modulo. Alla fine di questo percorso, specificare la nuova pagina di inizio per la scheda Report (start_page).

   ```
   $cgi?SID=$SESSION.SID+FID=123+OP=DISPLAY_FORM+HTMPL=show_report_frames.ht
   mpl+KEEP.report_form=start_page
   ```

   Fare clic su Salva.

   Viene visualizzata la pagina di inizio InfoView nella pagina Elenco Moduli Web.

Fase 7: Assegnazione della pagina iniziale del pulsante InfoView al record della scheda Report

In Gestione ruoli, assegnare la pagina iniziale del pulsante InfoView creata nella fase 6 al record della scheda Report.

Per assegnare la pagina iniziale del pulsante InfoView al record della scheda Report:

1. Selezionare il nuovo record di modulo Web della scheda Report dalla pagina Elenco tabelle in Gestione ruoli.

   Viene visualizzata la pagina dei dettagli.

2. Selezionare Modifica.

   Viene visualizzata la pagina Aggiorna scheda.

3. Specificare la nuova pagina iniziale del pulsante InfoView nel campo Pagina di avvio.

4. Fare clic su Salva.

   Quando un utente apre la scheda Report, il pulsante InfoView viene visualizzato nell'angolo in alto a destra del modulo.

Report basati sul Web

CA Business Intelligence installa una serie di report predefiniti basati sul Web per CA SDM e Gestione della conoscenza. Vengono sviluppati con BusinessObjects Enterprise Web Intelligence o con Crystal Reports. I report possono essere utilizzati come modelli per definire report specifici in base ai siti.

Questi report sono contenuti in cartelle che vengono distribuite automaticamente al server di reporting CA Business Intelligence dopo l'installazione.

È possibile assegnare un livello di protezione a cartelle e documenti per specificare se l'accesso è consentito a livello globale, per ruoli specifici o per singoli individui.

Nota: BusinessObjects InfoView include una Guida per l'utente che descrive l'utilizzo di BusinessObjects InfoView. Per accedere alla Guida dell'utente, fare clic sull'icona della guida in linea di InfoView. Per informazioni generali sull'uso di report predefiniti, consultare la *Guida in linea.*

Ulteriori informazioni:

Interfaccia di BusinessObjects InfoView (a pagina 887)
Spostamento tra i report (a pagina 888)
Preferenze di InfoView (a pagina 888)
Pianificazione dei report (a pagina 888)
Impostazione dell'analisi dei dati (a pagina 889)
Pubblicazione e distribuzione dei report (a pagina 890)

Interfaccia di BusinessObjects InfoView

Nella scheda Report CA SDM, analisti e gestori possono lavorare con report definiti per il proprio ruolo o gestire report personali facendo clic sul pulsante InfoView. Da InfoView, gli utenti possono accedere ai documenti Crystal Reports e Web Intelligence e ad altri oggetti, così da poterli organizzare a seconda delle esigenze.

Le funzionalità disponibili in InfoView variano in base al tipo di contenuto, ma in termini generali, è possibile visualizzare informazioni nel browser Web, esportarle in altre applicazioni aziendali (come Microsoft Excel) e salvarle in un'ubicazione specifica.

Nota: le cartelle e gli oggetti che possono essere visualizzati in InfoView dipendono dal gruppo (ruolo) assegnato all'utente.

Spostamento tra i report

È possibile spostarsi tra le cartelle nel riquadro sinistro della finestra InfoView per visualizzare, pianificare, modificare o eseguire il report oppure per visualizzare la cronologia e le proprietà di un report.

Per visualizzare un report

1. Usare *uno* dei seguenti metodi per aprire InfoView:
   - Dalla scheda Report CA SDM, fare clic sul pulsante InfoView.
   - Dal menu Start, selezionare Tutti i programmi, BusinessObjects XI, BusinessObjects Enterprise, BusinessObjects Enterprise Java InfoView.

   Viene visualizzata la pagina iniziale InfoView.
2. Nel riquadro sinistro, spostarsi nella struttura delle cartelle-Public Folders/Report CA/CA SDM.
3. Fare clic sulla cartella corrispondente al tipo di report che si desidera visualizzare.
4. Fare clic sul nome del report per il tipo di informazioni che si desidera visualizzare.

   Il report viene visualizzato in BusinessObjects InfoView.

Preferenze di InfoView

Gli utenti possono impostare preferenze generali per specificare che InfoView deve avviarsi con una delle loro pagine dashboard personali create con lo strumento My InfoView di Web Intelligence. Possono impostare anche le preferenze di visualizzazione di Web Intelligence e Crystal Reports.

Pianificazione dei report

InfoView supporta la pianificazione dei report. Per il reporting ad hoc, i report pianificati sono memorizzati nella sezione Cartelle. Se un report è impostato su "Aggiorna all'apertura", il sistema accede al database per ottenere le informazioni più recenti ogni volta che l'utente finale visualizza il report. Gli utenti possono pianificare l'esecuzione dei report ad orari specifici.

Gli amministratori possono definire calendari che riflettano date di pianificazione appropriate. Ad esempio, un utente può selezionare un calendario mediante l'opzione "Quando" (per orario e frequenza) in modo da visualizzare i giorni lavorativi disponibili, ignorando quelli non lavorativi.

Nota: per ulteriori informazioni sulla pianificazione di report, consultare la documentazione di BusinessObjects.

Tramite la pianificazione, gli utenti possono:

- Specificare l'orario e la frequenza delle pianificazioni (ad esempio immediata, oraria, giornaliera e settimanale)
- Specificare la destinazione, come una cartella di posta in arrivo, un'ubicazione file o un destinatario di posta
- Indicare a quali cartelle di posta in arrivo deve essere inviato il report
- Specificare l'output, come Web Intelligence, Crystal Report, Microsoft Excel e Adobe Acrobat
- Specificare le opzioni per l'inserimento nella cache Per impostazione predefinita, i risultati del documento vengono memorizzati sul server repository del file di output. Gli utenti possono tuttavia scegliere di configurare il sistema in modo che inserisca il report nella cache del server report di Web Intelligence selezionando un formato di cache e un locale.
- Selezionare il gruppo di server che elaborerà la richiesta. Se si seleziona un evento specifico, l'oggetto viene eseguito solo quando si verifica la condizione o l'evento aggiuntivi.

Nota: se si utilizzano partizioni dati CA SDM per gestire le restrizioni nella sezione della cartella pubblica di InfoView, è necessario definire i report pianificati contenuti nelle cartelle pubbliche per ciascun utente.

Impostazione dell'analisi dei dati

Un visualizzatore interattivo fornisce una vasta gamma di strumenti per adattare la visualizzazione dei dati dei report. È possibile analizzare in dettaglio i dati, da quelli dei gruppi fino a quelli degli assegnatari o delle richieste effettive.

I visualizzatori interattivi consentono di effettuare quanto segue:

- Modificare l'aspetto del report, visualizzando i dati in un formato diverso, come un grafico a torta. Ad esempio, se si fa clic con il pulsante destro del mouse sul report e si seleziona "Modifica tabella in", compaiono le funzioni per la presentazione dei report.
- Eseguire varie attività, come l'ordinamento, la creazione di interruzioni del report, il calcolo, il filtro e la classificazione del report.
- Condividere le informazioni con altri utenti e gruppi.

Pubblicazione e distribuzione dei report

Gli utenti di InfoView possono salvare i dati dei report in formato Excel, PDF o CSV, quindi distribuirli a una posizione di file, in una casella di posta in arrivo, a un indirizzo di posta elettronica o a un sito FTP.

Se un report viene approvato per essere utilizzato in CA SDM, viene spostato nella sezione pubblica, diventando così disponibile per gli utenti autorizzati. È possibile assegnare un livello di protezione a cartelle e documenti per specificare se l'accesso è consentito a livello globale, per ruoli specifici o per singoli individui. La protezione è amministrata nella console di gestione centralizzata di BusinessObjects.

Indicatori di prestazioni chiave

Gli *indicatori delle prestazioni chiave* (KPI) possono essere utilizzati per identificare aree dell'ambiente di gestione dei servizi che richiedono attenzione da parte dell'amministratore o l'ottimizzazione della configurazione.

Utilizzare l'interfaccia Web CA SDM per configurare le proprie definizioni KPI. I dati prodotti vengono memorizzati nel database CA SDM e sono disponibili per la creazione di report basati sul Web (a pagina 887).

Nota: in aggiunta alla definizione di query KPI, è possibile configurare il daemon KPI per recuperare dati di ticket CA SDM ad ogni apertura o chiusura di ticket, oltre che alla modifica di certi campi.

Definendo e controllando un gruppo di KPI pianificati, è possibile valutare il progresso verso il raggiungimento delle prestazioni desiderate nella propria organizzazione e raccogliere dati utili per prendere decisioni strategiche relative all'ambiente IT.

Nota: per informazioni sulle tabelle del database KPI, consultare la *Guida di riferimento tecnico*.

Tipi di KPI

CA SDM supporta tre tipi di KPI:

- I **KPI di sistema** vengono installati assieme al prodotto. È possibile personalizzarli per soddisfare le proprie esigenze, ma non crearne di nuovi.
- I **KPI di query memorizzate** richiamano una query memorizzata per recuperare metriche dal database. È possibile creare KPI di query memorizzate personalizzati o modificare gli esempi predefiniti installati con il prodotto.
- I **KPI SQL** consentono di incorporare una query SQL completa direttamente nel KPI. È possibile creare KPI SQL personalizzati o modificare gli esempi predefiniti installati con il prodotto.

Note:

- Per dettagli sulla configurazione di tutti e tre i tipi di KPI, vedere la *Guida in linea*.
- I KPI, predefiniti o creati dall'utente, non possono essere eliminati. Quando un KPI non è più necessario, è possibile disattivarlo impostando lo stato del record su inattivo.

KPI predefiniti

Diversi KPI di ciascun tipo vengono installati con CA SDM. Potrebbe essere utile esaminarli mentre si legge la presente guida.

È possibile utilizzare la query memorizzata e i KPI SQL con le definizioni originali oppure come modelli per le definizioni personalizzate.

È possibile utilizzare i KPI di sistema predefiniti con le definizioni originali oppure modificare alcuni dei campi per soddisfare le proprie esigenze.

Nota: la maggior parte dei KPI predefiniti sono impostati sullo stato di inattivi per impostazione predefinita. Per visualizzarli nell'interfaccia Web, filtrare la pagina Elenco KPI per visualizzare i KPI inattivi.

Daemon KPI

Il daemon KPI gestisce il recupero, l'organizzazione e l'archiviazione di dati metrici KPI. Il daemon viene eseguito in continuazione e raccoglie dati a intervalli specifici da diverse risorse di sistema.

Quando si raggiunge il momento dell'aggiornamento di un KPI, il daemon KPI interagisce con altri componenti di sistema nel modo seguente:

- **KPI di sistema**—Invia una richiesta a un daemon di destinazione (webengine, domsrvr, bpvirtdb o db_agents) per recuperare dati di conteggio o durata.
- **KPI di query memorizzate**—Invia una richiesta a domsrvr per ottenere dati di conteggio.
- **KPI SQL**—Invia una richiesta a domsrvr per ottenere dati di conteggio, somme, valori massimi o durate.

Quando il daemon KPI riceve i dati richiesti, memorizza le metriche risultanti nel database.

Nota: la durata calcolata è basata su una modifica dei valori in un ticket in tempo reale, non in orario lavorativo.

KPIs sistema

I KPI di sistema consentono di raccogliere dati metrici relativi all'operazione dei processi CA SDM.

Sono supportati i seguenti tipi di processo:

- **domsrvr**—Gestione oggetto CA SDM (processo server). Gestione oggetti memorizza inoltre nella cache vari record e tabelle per i client.
- **bpvirtdb** - Il server di database virtuale BOP consente l'operazione di più gestioni oggetto nell'ambiente di CA SDM. Le gestioni oggetto si connettono al database virtuale che ne arbitra l'accesso agli agenti di database. Ad esempio, quando viene recuperato un nuovo intervallo di numeri di riferimento di ticket, il database virtuale assicura il fatto che solo un gestore oggetto alla volta acceda alla tabella contenente i numeri di riferimento.

  A seconda della configurazione di CA SDM, le gestioni oggetto si connettono al database virtuale dei server seguenti:

  - Convenzionale: tutte le gestioni oggetto in esecuzione sul server primario o sul server secondario si connettono al database virtuale del server primario.
  - Disponibilità avanzata: tutte le gestioni oggetto si connettono al database virtuale dello stesso server su cui sono in esecuzione. Ad esempio, le gestioni oggetto in esecuzione sul server applicazioni si connettono al database virtuale solo del server applicazioni.

  Il database virtuale effettua anche la memorizzazione nella cache di informazioni di database per Gestione oggetto.

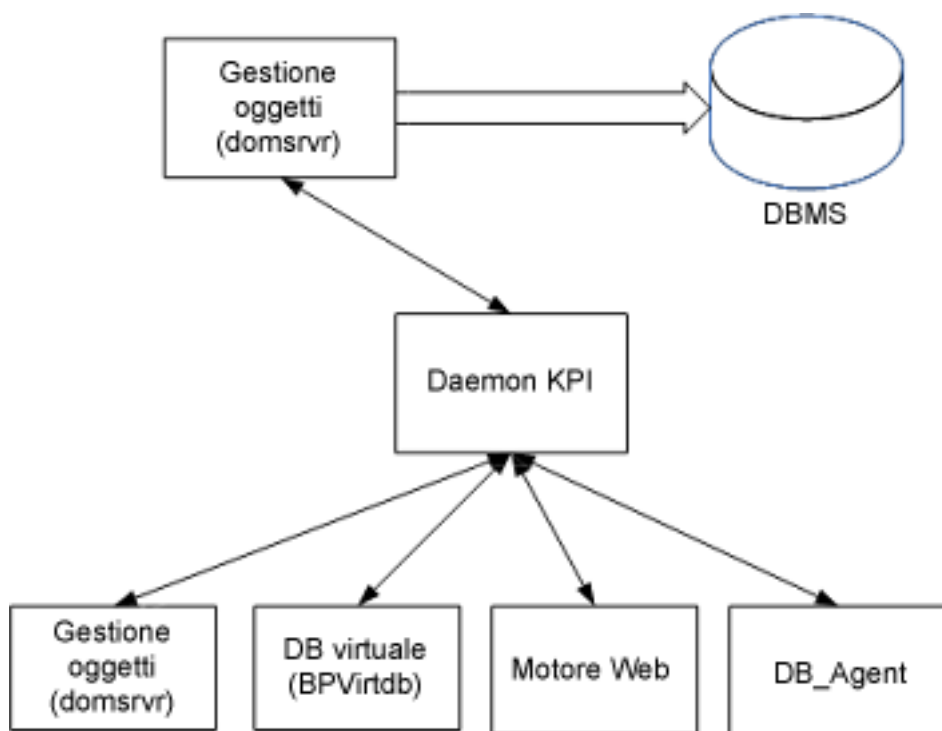
- **db_agents**—Gli agenti di database eseguono query SQL e gestiscono altre interazioni tra CA SDM e il sistema di gestione del database (DBMS). Gli agenti di database aderiscono allo schema di database CA SDM e traducono il codice SQL nella forma richiesta dal DBMS particolare (ad esempio, Oracle).
- **webengine**—Il componente CA SDM che collega browser Web a un gestore oggetti attraverso un pdmweb cgi eseguito in un server Web Microsoft IIS o Apache Tomcat.

  A seconda della configurazione di CA SDM, è necessario un motore Web per WSP sui server seguenti affinché la Progettazione schema WSP esegua la scrittura dei file di schema:

  - Convenzionale: server primario
  - Disponibilità avanzata: server in background

  I motori Web sono i client effettivi di un gestore oggetti per i browser Web dei client degli utenti. Motori Web .htmpl della cache dei motori Web per utenti connessi. È possibile manipolare la cache utilizzando l'utilità pdm_webcache e visualizzare le statistiche relative alle connessioni dei client utilizzando l'utilità pdm_webstat.

Nota: per maggiori informazioni su questi processi, consultare la *Guida all'implementazione*.

Il diagramma riportato di seguito illustra il flusso dati per i KPI di sistema.

Ciascun KPI di sistema produce uno dei seguenti tipi di metrica:

- Numero
- Durata

Esempi di KPI di sistema

- Questo esempio produce un conteggio delle richieste di aggiornamento inviate al database virtuale BOP:

  ```
  updateCt
  ```

- Questo esempio riporta il tempo necessario al completamento delle richieste di aggiornamento, inserimento ed eliminazione al database virtuale BOP:

  ```
  virtdbUpdateResponseDt
  ```

KPI delle query memorizzate

I KPI delle query memorizzate consentono di generare report basati su metriche di conteggio recuperate dal database CA SDM.

Il database CA SDM offre una serie di query memorizzate predefinite. Molte di esse sono utili così come sono. È anche possibile personalizzarle per soddisfare le proprie esigenze oppure utilizzarle come modelli per scrivere le proprie query.

Tutti i KPI di query memorizzate dispongono di un tipo di metrica Conteggio.

Nota: è possibile utilizzare le query memorizzate per produrre campi contatore per il segnapunti dell'interfaccia Web o metriche KPI, oppure entrambi. Per utilizzare una query memorizzata in una definizione di KPI, è necessario attivare la query per l'uso di KPI. Per ulteriori informazioni, vedere Configurazione delle query memorizzate (a pagina 467).

Esempi di KPI di query memorizzate

- Questo esempio produce un conteggio degli ordini di cambiamento aperti nell'ubicazione dell'assegnatario:

  ```
  Modifiche @cnt.posizione.name
  ```

- Questo esempio produce un conteggio dell'attività del flusso di lavoro che violerà un SLA prima della mezzanotte del giorno corrente:

  ```
  Att flusso lav probl che violeranno uno SLA oggi
  ```

KPI SQL

I KPI SQL offrono maggiore flessibilità rispetto ai KPI della query memorizzata. Con i KPI SQL è possibile scrivere le proprie query nel database CA SDM per produrre i tipi seguenti di metrica:

- Somma
- Numero
- Massimo
- Durata

Nota: il codice SQL deve essere conforme alla sintassi SQL92.

Le considerazioni seguenti sono valide per i KPI SQL:

- Per vedere il codice SQL per queste query di esempio, aprire le definizioni della query dalla pagina Elenco KPI.

  Nota: per le istruzioni, consultare la *Guida in linea*.

- Il simbolo @ non è supportato nei KPI SQL. Utilizzare la sintassi indicata nell'esempio seguente e un alias di attributo:

  ```
  SELECT * FROM cr WHERE assignee_last_name = "Smith"
  ```

  Per questo esempio sarebbe stato possibile utilizzare un alias di attributo predefinito. Viene visualizzata la pagina dei dettagli dell'alias attributo.

  " Nome oggetto = cr

  " Nome alias = assignee_last_name

  " Stato = Attivo

  " Valore alias = assignee.last_name

Esempi: KPI con query SQL

- Questo esempio predefinito produce la somma dei costi stimati di tutte le attività del flusso di lavoro dell'ordine di cambiamento in sospeso:

  ```
  Somma dei costi stimati delle attività del flusso di lavoro con modifica in sospeso
  ```

- Questo esempio predefinito produce un conteggio degli ordini di cambiamento attivi che sono stati chiusi e riaperti:

  ```
  Conteggio degli ordini di cambiamento riaperti
  ```

Campi KPI

Nella seguente tabella vengono descritti i campi KPI. Le colonne Sys. S.Q. e SQL indicano i tipi di KPI a cui appartiene ciascun campo (Sistema, Query memorizzata o SQL).

Nota: tutti i campi sono obbligatori a meno che non vengano specificati come opzionali.

Campo	Sys.	S.Q.	SQL	Descrizione
Nome KPI	X	X	X	Identifica il nome visualizzato per il KPI. Non modificabile.
Tipo	X	X	X	Definisce il record come Sistema, Query memorizzata o KPI SQL. Non modificabile.
Mantieni versione esistente	X	X	X	Consente di specificare che, aggiornando il record, sarà mantenuta la versione corrente del record KPI. Modificabile quando l'impostazione @NX_ALWAYS_KEEP_KPI_VERSIONS in NX.env è impostata su N.
Versione	X	X	X	Identifica il numero di versione del record KPI. Il numero di versione viene incrementato automaticamente ad ogni aggiornamento del record. Non modificabile.
Stato record	X	X	X	Specifica se il KPI è attivo (raccolta dati) o inattivo (senza raccolta dati). Modificabile solo utilizzando la caratteristica "Modifica in elenco" nella pagina Elenco KPI.
Tipo di metrica	X	X	X	Consente di specificare il tipo di calcolo che verrà eseguito dal KPI. ■ I KPI della query memorizzata sono sempre Conteggio. ■ I KPI di sistema possono essere Conteggio o Durata. ■ I KPI SQL possono essere Conteggio, Somma, Massimo o Durata. Modificabile solo per KPI tipo SQL.
AggiornaOra	X	X	X	Specifica l'intervallo di tempo per il recupero di metriche KPI dal database. Il valore è modificabile. Il tempo di aggiornamento viene specificato nel formato HH:MM:SS.
Processo Tipo	X			Le metriche di KPI di sistema (a pagina 892) possono derivare dai seguenti processi CA SDM: ■ **domsrvr**—Gestione oggetti ■ **bpvirtdb**—Server di database virtuale BOP ■ **db_agents**—Agenti di database ■ **webengine**—Il client Web CA SDM

Campo	Sys.	S.Q.	SQL	Descrizione
Sistema Nome	X			Il nome interno del KPI di sistema. Non modificabile.
Utente Contesto		X	X	(Facoltativo) Consente di specificare l'ID utente di un contatto CA SDM. Le assegnazioni di ruolo e titolare del contatto sono utilizzate per determinare la partizione dati della metrica prodotta dal KPI. Il valore è modificabile.
Archiviato Query		X		Il nome della query archiviata richiamata da questo KPI. Il valore è modificabile.
SQL Query			X	Il codice SQL per la query. Il valore è modificabile.
Descrizione	X	X	X	(Facoltativo) Fornisce una descrizione dettagliata del KPI. Il valore è modificabile.

Recupero dei dati del ticket

Per consentire il reporting di quanto tempo i ticket devono rimanere nei vari stati di elaborazione, è possibile configurare il daemon KPI in modo che recuperi i dati dei ticket <USDK> quando un ticket viene aperto o chiuso e ogni volta che vengono modificati i valori dei seguenti campi:

- Attivo
- Assegnatario
- Area o categoria
- Gruppo
- Impact
- Organizzazione
- Priorità
- Causa principale
- Stato
- Tipo di servizio

Per attivare il recupero dei ticket, installare l'opzione Tabella dei dati ticket KPI, disponibile nella cartella KPI Gestione opzioni.

Viene attivata la raccolta dei dati dai ticket nuovi e aggiornati. Il data ticket è scritto nella tabella di database usp_kpi_ticket_data ed è disponibile per la generazione dei report basati sul Web.

Nota: per le istruzioni, consultare la *Guida in linea*.

Le considerazioni seguenti sono valide per il recupero dei ticket:

- Il daemon KPI può richiedere fino a 30 minuti per compilare le informazioni del ticket nella tabella usp_kpi_ticket_data.
- Il campo support_lev consente di tenere traccia dell'elaborazione del tipo di servizio se è installata l'opzione classic_sla_processing. L'opzione classic_sla_processing consente l'elaborazione del Tipo servizio da CA SDM versione 6.0 e precedente.
- L'abilitazione di questa funzione potrebbe pregiudicare le prestazioni di CA SDM.

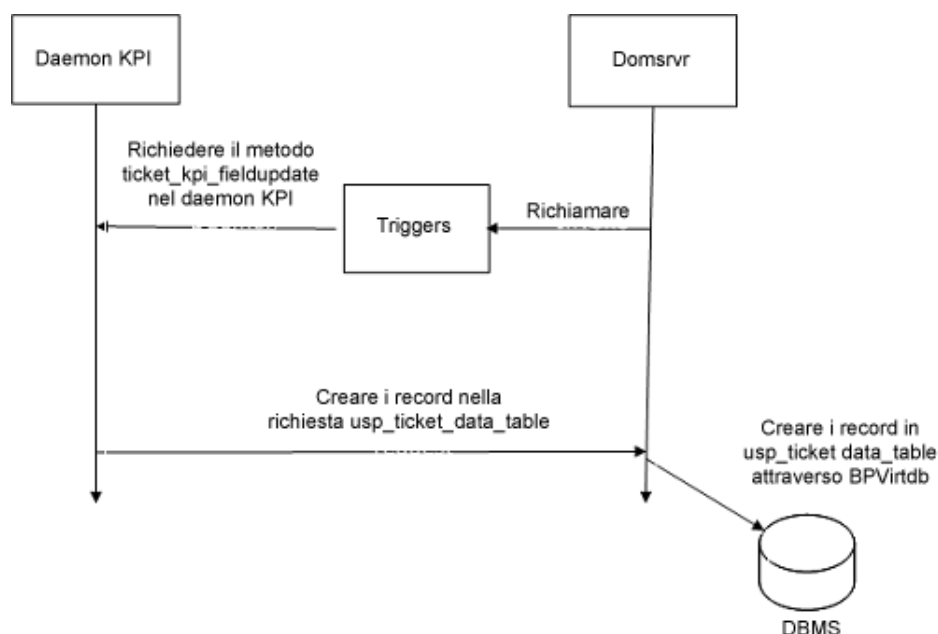
Ulteriori informazioni:

File NX.env (a pagina 901)

Flusso di dati di ticket KPI:

L'opzione Tabella dei dati ticket KPI si basa su un meccanismo di trigger. Quando è installata l'opzione kpi_ticket_data_table, il daemon KPI inizia a monitorare oggetti di ticket CA SDM per tenere traccia degli eventi seguenti:

- Apertura di un nuovo ticket
- Controllo di modifiche a uno o più campi monitorati
- Chiusura di un ticket

Quando si verifica uno di questi eventi, viene attivato un trigger POST_CI. Il trigger invia un BPMessage con un elenco di attributo di trigger al daemon KPI, aggiungendo i dati restituiti alla tabella usp_kpi_ticket_data, come illustrato nel seguente diagramma di flusso dei dati.

Tipi di record di tabella dei dati del ticket KPI

Sono disponibili cinque tipi di operazione nella tabella usp_kpi_ticket_data:

- INIT (0)
- NO_INIT_REC (1)
- REOPEN (2)
- UPDATE (3)
- CLOSE (4)

Il valore tipo (valore intero mostrato in parentesi) viene memorizzato nel campo operativo. Il campo end_time del record precedente viene memorizzato nel campo prev_time. Il campo ktd_duration memorizza la durata, calcolata come end_time meno prev_time. Il record precedente viene definito nelle regole seguenti:

1. Il record INIT indica che è stato creato un ticket.
2. Viene creato un record UPDATE per ciascun aggiornamento di ticket. Ottiene prev_time da un precedente record UPDATE allo stesso campo ticket se esiste un precedente record UPDATE. Altrimenti ottiene prev_time dal record INIT, NO_INIT_REC o REOPEN, a seconda del record che dispone di un valore end_time più vicino nel tempo al record UPDATE.
3. Il record CLOSE è lo stesso di UPDATE.
4. Se viene riaperto un ticket, viene creato un singolo record REOPEN per mostrare il valore del campo Attivo. Il record REOPEN ottiene prev_time da un precedente record CLOSE per lo stesso campo Attivo.
5. Se è stato creato un ticket prima di attivare l'opzione Gestione opzioni, è possibile che siano presenti record di aggiornamenti ma senza un record INIT. Il programma in questo caso crea un record NO_INIT_REC e ottiene prev_time dal primo record non-INIT incontrato.

Nota: per la documentazione completa dei campi della tabella, consultare la *Guida di riferimento tecnico*.

Risoluzione dei problemi

È possibile diagnosticare gli eventuali problemi durante l'uso dei KPI.

Verificare che il daemon KPI sia in esecuzione.

Per verificare che il daemon KPI sia in esecuzione, eseguire l'utilità pdm_status della riga di comando nel modo seguente:

```
pdm_status
```

Esaminare l'output seguente:

```
KPI Daemon myserver  Running  myserver 3568  Wed Feb 06 07:23:53
```

File NX.env

Esaminare il file $NX_ROOT/NX.env per verificare che la configurazione KPI di base sia stata impostata correttamente.

Se è stata installata l'opzione della tabella dei dati del ticket KPI, il file NX.env include quanto segue:

```
######################################################################
# NX_KPI_TICKET_DATA_TABLE
# Attiva la raccolta di campi modificati da oggetti ticket
# (come Richieste, Issue e Ordini di cambiamento) per scrivere voci di record
# nella tabella usp_kpi_ticket_data.
######################################################################
@NX_KPI_TICKET_DATA_TABLE=Yes

######################################################################
# NX_KPI_FUZZ_TIME
# Specifica un ritardo tollerabile per ciascun KPI all'interno del quale kpi_daemon
# invia una richiesta per recuperare dati KPI quando il tempo di aggiornamento di questo
kPI
# è in timeout
######################################################################
@NX_KPI_FUZZ_TIME=20
```

Nota: il valore predefinito di @NX_KPI_FUZZ_TIME è 20. È possibile modificare questo valore all'interno dell'intervallo da 0 a 40 secondi. Se si imposta questa variabile per un valore maggiore di 40, verranno utilizzati 40 secondi.

```
######################################################################
# NX_ALWAYS_KEEP_KPI_VERSIONS
# L'attributo keep_version nella tabella Kpi viene visualizzato nel modulo di
# modifica dei dettagli come casella di controllo. L'opzione
NX_ALWAYS_KEEP_KPI_VERSIONS
# specifica che la casella di controllo è di sola lettura ed è sempre selezionata.
######################################################################
@NX_ALWAYS_KEEP_KPI_VERSIONS=Yes
```

Attivazione del tracciamento daemon KPI

Utilizzare l'utilità pdm_logstat per attivare la registrazione delle tracce per il monitoraggio dell'attività del daemon KPI.

Per attivare il tracciamento del daemon KPI, eseguire il comando seguente:

```
pdm_logstat -f cache_table_mgr.c VERBOSE
```

Per disattivare il tracciamento del daemon KPI, eseguire il comando seguente:

```
pdm_logstat -f cache_table_mgr.c
```

Esaminare il file stdlog.0 per le voci appartenenti all'attività del daemon KPI.

L'esempio seguente mostra normali connessioni daemon KPI al computer host e il comando domsrvr:

```
02/06 05:42:14,58 garbo-2k3-bb kpi_daemon 2432 SIGNIFICANT kpi_daemon.c  117 KPIDaemon ready for action!
02/06 05:42:14,80 garbo-2k3-bb domsrvr 792 SIGNIFICANT connmgr.c 2314 Connecting client kpi_daemon:garbo-2k3-bb
02/06 05:42:14,81 garbo-2k3-bb kpi_daemon 2432 SIGNIFICANT main.c 220 KPI daemon connected with domsrvr
```

L'esempio seguente indica un errore in un KPI denominato webSessionCT:

```
01/16 13:24:46,74 jed web:local 2152 ERROR sys_kpi.c 96 Invalid KPI metric type: 1382180215 (KPI name:webSessionCT)
```

Gli esempi seguenti mostrano l'attività del daemon KPI:

```
02/06 07:23:50,47 garbo-2k3-bb kpi_daemon 3568 TRACE cache_table_mgr.c 427 Cache Table manager created Kpi_Obj (KPI dob record_id:9003) (KPI type:2)
02/06 07:23:50,53 garbo-2k3-bb kpi_daemon 3568 TRACE cache_table_mgr.c 427 Cache Table manager created Kpi_Obj (KPI dob record_id:9103) (KPI type:1)
```

Nota: per informazioni sui tipi di KPI, vedere Tipi di record di tabella dei dati del ticket KPI (a pagina 899).

Report ad hoc

I report ad hoc vengono sviluppati in InfoView utilizzando Web Intelligence. È possibile creare report ad hoc.

Nota: per ulteriori informazioni sui report ad hoc, consultare la documentazione di BusinessObjects Enterprise. Per accedere alla documentazione, fare clic sull'icona della guida in linea di InfoView.

Interfaccia Web Intelligence

In InfoView, Web Intelligence offre uno strumento di reporting personalizzato, destinato agli utenti che desiderano creare report di base in modo semplice e senza scrivere query. I report in Web Intelligence offrono modelli predefiniti per gestire connessioni dati, query e relazioni dati; in questo modo, è sufficiente trascinare i campi dati su un modello per creare report in formato tabellare o matrice. È possibile utilizzare tutte le funzioni di InfoView descritte nella *Guida dell'utente di InfoView*.

Un documento Web Intelligence fa riferimento a un oggetto BusinessObjects, definito universo, per la creazione di report. I nuovi report vengono creati in universi BusinessObjects. CA Business Intelligence offre, insieme al prodotto, l'universo CA SDM.

Funzionamento del reporting ad hoc

Il reporting ad hoc funziona come descritto di seguito:

1. Per avviare un report ad hoc, è necessario prima selezionare l'universo CA SDM in InfoView.
2. L'universo è associato al database CA SDM in cui sono contenute informazioni aziendali. Quando ci si collega a un universo, in Web Intelligence viene automaticamente avviato l'editor di documenti selezionato nella pagina Web Intelligence Document Preferences di InfoView.

   Nota: per informazioni sulle preferenze di impostazione, vedere la *Guida dell'utente di InfoView*.

3. È possibile usare l'universo per creare query e recuperare i dati da usare in un report utilizzando gli oggetti raggruppati in cartelle chiamate classi. Ogni classe può contenere anche una o più classi secondarie. Le sottoclassi contengono oggetti che sono a loro volta una sottocategoria degli oggetti presenti nella classe di livello superiore. Classi e oggetti vengono presentati in una struttura ad albero (gerarchia) nella scheda Data.

   Nota: per istruzioni su come creare le query per i documenti di Web Intelligence, vedere la documentazione di BusinessObjects Enterprise.

4. Una volta creata la query, è possibile eseguire la query aggiungendo gli oggetti richiesti al riquadro Result Objects (Oggetti risultato) e le proprietà delle query definite. Quando si esegue una query, l'universo chiede al database di recuperare i dati che corrispondono alle richieste di ciascuno degli oggetti presenti nella query. Per eseguire una query, fare clic su Run Query nella barra degli strumenti.

   Importante. quando si selezionano gli oggetti per la query, scegliere sempre oggetti, misure e filtri solo da una classe di base degli universi e dalle sue sottoclassi. Se si includono oggetti, misure e filtri di più classi di base di universi in una query, è possibile che i risultati non siano quelli attesi e che le prestazioni siano insoddisfacenti.

Esempio di report ad hoc

È possibile utilizzare Web Intelligence e gli esempi di query per creare report ad hoc utilizzando l'universo CA SDM predefinito. Quando si crea un report, assicurarsi di salvarlo a intervalli regolari. Se la sessione di connessione a Web Intelligence scade, le modifiche al report andranno perse.

Nota: per informazioni sulla modifica del valore di timeout della sessione, consultare la *Guida all'implementazione*.

Esempio: visualizzazione di tutte le richieste con priorità aperta 1 e 2 per tutti gli utenti

In questo esempio, è necessario specificare i valori di prompt speciali per acquisire dati aggiuntivi prima di generare il report.

Esempio: visualizzazione di tutte le richieste con priorità aperta 1 e 2 per tutti utenti

1. Fare clic su New, Web Intelligence Document nella barra dei menu.

   Viene visualizzata la pagina New Web Intelligence Document.

2. Selezionare l'universo CA SDM nella colonna Universe.

   Il documento Web Intelligence viene visualizzato insieme alle informazioni relative all'universo nel riquadro sinistro.

   Nota: per migliorare la navigazione, chiudere la cartella Attached Service Type (Tipo servizio associato) nel riquadro sinistro.

3. Individuare ed espandere le cartelle Request, Request Detail nel riquadro di sinistra. Usare la barra di scorrimento per trovare le cartelle.

4. Selezionare ciascuno degli oggetti seguenti, quindi trascinarli e rilasciarli dal riquadro sinistro al riquadro in alto a destra negli oggetti risultanti.

   - Riepilogo
   - Simbolo di priorità
   - Customer Combo Name (Nome combinato cliente)

5. Selezionare ciascuno dei seguenti oggetti e trascinarli nel riquadro in basso a destra sotto a Query Filters (Filtri query). Al termine, chiudere la cartella Request Detail.

   - Simbolo di stato
   - Simbolo di priorità

6. Espandere la cartella Request Filters (Filtri richiesta), quindi trascinare e rilasciare il nome combinato del cliente con il filtro Userid (ID utente) nel riquadro in basso a destra sotto a Query Filters (Filtri Query).

7. Nel riquadro Query Filters (Filtri query), fare clic sulla freccia In list (In elenco) nel filtro del simbolo di stato e selezionare l'operatore Equal (Uguale).

8. Selezionare i valori dal menu Operand Type (Tipo di operando).

   Viene visualizzato l'elenco della finestra di dialogo dell'elenco dei valori.

9. Nell'elenco dei simboli di stato, selezionare Open (Apri), quindi fare clic sulla freccia verde.

   Il valore viene visualizzato nel campo Value(s) Selected (Valori selezionati).

10. Fare clic su OK.

11. Nel riquadro Query Filters (Filtri query), fare clic sulla freccia In list (In elenco) nel filtro del simbolo di priorità e selezionare l'operatore In list (In elenco).
12. Nell'elenco dei simboli di priorità, selezionare contemporaneamente 1 e 2, quindi fare clic sulla freccia verde.

    I valori 1 e 2 vengono visualizzati nel campo Value(s) Selected (Valori selezionati).
13. Fare clic su OK.
14. Fare clic su Run Query nella barra degli strumenti per generare il report.

    Nota: poiché il nome combinato cliente con il filtro rapido Userid (ID utente) utilizza la funzione Prompt, viene visualizzata la finestra di dialogo Prompts (Prompt). Questa finestra di dialogo consente di raccogliere dati aggiuntivi prima della creazione del report.
15. Nella finestra Prompts (Prompt), selezionare la prima opzione, ALL (Tutto), quindi fare clic sul pulsante freccia verde.

    Tutti i nomi degli utenti vengono visualizzati nell'elenco Select Customer (Selezione cliente).
16. Fare clic su Run Query per generare il report.

    Il report compare in una nuova finestra.
17. Fare doppio clic sul titolo del report e digitare Priority 1 & 2 Open Requests for All Users nella casella di testo. È possibile modificare il formato del carattere in 16 o in un altro formato.
18. Per modificare altri aspetti del report, fare clic sulla scheda Properties (Proprietà).
19. Per creare sottogruppi dei dati utilizzando il cognome del cliente, fare clic con il pulsante destro del mouse su qualsiasi cella dati nella colonna Customer Last Name (Cognome cliente), quindi selezionare Set as Section (Imposta come sezione).
20. Fare clic su Save e specificare una posizione mediante l'opzione Save As.

Esempio: visualizzazione di tutte le richieste che non includono lo stato Work In Progress

In questo esempio, viene specificata la funzione di reporting Conteggio per restituire il numero totale di richieste aperte.

Esempio: visualizzazione di tutte le richieste che non includono lo stato Work In Progress

1. Fare clic su New, Web Intelligence Document nella barra dei menu.

    Viene visualizzata la pagina New Web Intelligence Document.

2. Selezionare l'universo CA SDM nella colonna Universe.

   Il documento Web Intelligence viene visualizzato insieme alle informazioni relative all'universo nel riquadro sinistro.

   Nota: per migliorare la navigazione, chiudere la cartella Attached Service Type (Tipo servizio associato) nel riquadro sinistro.

3. Individuare ed espandere le cartelle Request, Request Detail nel riquadro di sinistra. (Usare la barra di scorrimento per spostarsi tra le cartelle).
4. Selezionare ciascuno degli oggetti seguenti, quindi trascinarli e rilasciarli dal riquadro sinistro al riquadro in alto a destra negli oggetti risultanti.
   - Simbolo di stato
   - N. rif.
   - Riepilogo
5. Selezionare l'oggetto Status Symbol (Simbolo di stato), quindi trascinarlo e rilasciarlo nel riquadro in basso a destra sotto a Query Filters (Filtri query). Chiudere la cartella Dettagli Richiesta.
6. Espandere la cartella Request Filters (Filtri richiesta), quindi trascinare e rilasciare il filtro attivo nel riquadro in basso a destra sotto a Query Filters (Filtri query).
7. Nel riquadro Query Filters (Filtri query), fare clic sulla freccia In list (In elenco) nell'oggetto Status Symbol (Simbolo di stato) e selezionare l'operatore Not Equal (Non uguale).
8. Selezionare Work In Progress dal menu Operand Type.
9. Fare clic su Edit Report nella barra degli strumenti principale.

   Viene visualizzato il visualizzatore di report.

10. Selezionare la colonna Ref Num nel report. Questa azione attiva il comando Insert Sum nella barra degli strumenti di reporting.
11. Fare clic sul comando Insert Sum, quindi selezionare Count dal menu.
12. Nel report, fare clic con il pulsante destro del mouse sulla cella =[Status Symbol], quindi selezionare Set as Section dal menu di scelta rapida.
13. Fare clic su Refresh Data (Aggiorna dati) sulla barra degli strumenti principale per eseguire il report.
14. Fare clic su Salva.

    Il report mostra il numero totale (conteggio) di richieste che *non* hanno lo stato Work in Progress.

Esempio: visualizzazione di tutte le richieste chiuse negli ultimi 30 giorni per gli utenti il cui cognome inizia con "C"

In questo esempio è necessario specificare valori di prompt per la data di chiusura e il cognome del cliente in modo che vengano restituite tutte le richieste chiuse basate su questi valori.

Esempio: visualizzazione di tutte le richieste degli ultimi 30 giorni per gli utenti il cui cognome inizia con "C"

1. Fare clic su New, Web Intelligence Document nella barra dei menu.

   Viene visualizzata la pagina New Web Intelligence Document.

2. Selezionare l'universo CA SDM nella colonna Universe.

   Il documento Web Intelligence viene visualizzato insieme alle informazioni relative all'universo nel riquadro sinistro.

   Nota: per migliorare la navigazione, chiudere la cartella Attached Service Type (Tipo servizio associato) nel riquadro sinistro.

3. Individuare ed espandere le cartelle Request, Request Detail nel riquadro di sinistra. Usare la barra di scorrimento per spostarsi tra le cartelle.

4. Selezionare ciascuno degli oggetti seguenti, quindi trascinarli e rilasciarli dal riquadro sinistro al riquadro in alto a destra negli oggetti risultanti.

   - N. rif.
   - Data di chiusura
   - Cognome cliente
   - Riepilogo

5. Selezionare ciascuno dei seguenti oggetti e trascinarli nel riquadro destro sotto a Query Filters (Filtri query).

   - Simbolo di stato
   - Data di chiusura
   - Cognome cliente

6. Fare clic sulla freccia In list (In elenco) nel filtro Simbolo di stato e selezionare i valori dall'elenco del menu Operand Type (Tipo di operando).

   Viene visualizzato l'elenco della finestra di dialogo dell'elenco dei valori.

7. Selezionare i seguenti valori nell'elenco dei simboli di stato:

   - Chiuso
   - Chiuso-non risolto

- Chiusura richiesta
- Problema-Chiuso
- Problema-Corretto
- Risolto

8. Fare clic sulla freccia verde.

   I valori vengono visualizzati nel campo Value(s) Selected (Valori selezionati).

9. Fare clic su OK.
10. Nel riquadro Query Filters, fare clic sulla freccia verde nell'oggetto Close Date e selezionare l'operatore Between.
11. Fare clic sulla freccia In list e selezionare Prompt dal primo e secondo menu Operand Type (Tipo di operando).
12. Fare clic sulla freccia In list (In elenco) nell'oggetto Customer Last Name (Cognome cliente) e selezionare l'operatore Matches pattern (Corrispondenza schema).
13. Fare clic sulla freccia In list (In elenco) e selezionare Prompt dal menu Operand Type (Tipo di operando).
14. Fare clic sull'icona delle proprietà del prompt visualizzata vicino alla freccia In list (In elenco).

    Viene visualizzata la finestra di dialogo Prompt.

15. Nel campo di testo Prompt, immettere uno schema per il cognome cliente.
16. Fare clic su OK.
17. Fare clic su Run Query nella barra degli strumenti per generare il report.

    Nota: poiché gli oggetti Close Date e Customer Last Name utilizzano la funzione Prompt, viene visualizzata la finestra di dialogo Prompts. Questa finestra di dialogo consente di raccogliere dati aggiuntivi prima della creazione del report.

18. Nella finestra Prompts (Prompt), selezionare o immettere i valori di prompt per ciascuno dei seguenti elementi:
    - Enter Close Date (Start) (Immettere la data di chiusura (inizio): specificare una data che preceda di 30 giorni la data odierna.
    - Enter Close Date (End) (Immettere la data di chiusura (fine): specificare la data odierna.
    - Immettere uno schema per il cognome cliente: specificare C%.
19. Fare clic su Run Query per generare il report.

    Il report compare in una nuova finestra.

20. Fare doppio clic sul titolo del report e digitare nella casella di testo View All Closed Requests in Last 30 Days for Users Whose Last Name Begins with "C". È possibile modificare il formato del carattere in 16 o in un altro formato.

21. Per modificare altri aspetti del report, fare clic sulla scheda Properties (Proprietà).
22. Fare clic su Save e specificare una posizione mediante l'opzione Save As.

Report del dashboard

È possibile utilizzare il reporting del dashboard per monitorare le operazioni quotidiane per tutti i tipi di ticket di CA SDM (Richiesta/Incidente/Problema, Ordine di cambiamento o Issue) Gestione della conoscenza, Support Automation e CMDB in BusinessObjects InfoView. Ciascun report contiene informazioni analitiche sulle migliori prestazioni su ticket attivi, in modo da poterne seguire l'andamento.

Il reporting del dashboard consente di eseguire le operazioni seguenti:

- Visualizzare informazioni di riepilogo e dettagliate sui ticket attivi suddivisi per priorità, analista, categoria o gruppo.
- Determinare il numero di ticket risolti in un periodo di tempo e altre informazioni.
- Modificare, stampare, tenere traccia e salvare report in altri formati, ad esempio .xls e .pdf.

È possibile utilizzare report di dashboard predefiniti individuali oppure il dashboard aziendale per includere tutte le operazioni giornaliere di CA SDM in un'unica visualizzazione. Il dashboard aziendale contiene informazioni importanti sulle operazioni quotidiane per tutti i tipi di ticket (Richiesta/Incidente/Problema, Ordine di cambiamento o Richiesta) suddivisi per priorità, analista, categoria o gruppo.

Nota: quando si utilizza il reporting del dashboard, sono disponibili le funzionalità di InfoView descritte nella sezione Working with Dashboard and Analytics della guida *BusinessObjects Enterprise InfoView User's Guide*. Per accedere alla Guida dell'utente, fare clic sull'icona della guida in linea di InfoView.

Visualizzazione di dashboard e report in InfoView

L'utente con account amministratore può accedere e visualizzare i report in BusinessObjects InfoView. Le cartelle e i report disponibili in InfoView dipendono dall'account utilizzato per l'accesso e dalle autorizzazioni concesse a tale account.

Per eseguire la verifica dei report di dashboard in InfoView:

1. Accedere a CA SDM.
2. Dalla scheda Report , fare clic sul pulsante InfoView.

   InfoView viene visualizzato nel browser Web.
3. Nella barra degli strumenti di InfoView, selezionare Elenco Documenti.

   Nell'area di navigazione vengono visualizzati cartelle e oggetti.

4. Selezionare Public Folders, CA Reports, CA SDM Dashboards.

   Verranno visualizzate le cartelle seguenti: Ordine di cambiamento, Incidente, Questione, Problema, Richiesta, Configurazione e Conoscenza.

5. Selezionare il report appropriato.

   Il report selezionato viene visualizzato nel riquadro destro.

6. Fare doppio clic sul titolo per visualizzare un report.

   Il report viene aperto per la visualizzazione.

Scrivere report di CA Business Intelligence

È possibile scrivere report di CA Business Intelligence per CA SDM.

Ulteriori informazioni:

Driver ODBC CA SDM (a pagina 910)
Stesura rapporti SQL per BusinessObjects (a pagina 911)
Funzioni PDM (a pagina 912)
Alias attributi (a pagina 914)
pdm_isql Interactive SQL (a pagina 914)

Driver ODBC CA SDM

Le applicazioni di reporting di BusinessObjects (Crystal Reports e Web Intelligence) accedono ai dati utilizzando un driver ODBC che li collega direttamente al motore oggetti di CA SDM chiamato domsrvr.

Questa connessione fornisce una serie di vantaggi:

- Istruzioni SELECT utilizzate dagli oggetti e dagli attributi di riferimento dei report di BusinessObjects che usano i propri nomi CA SDM (in altre parole, i nomi Majic). Per esempio, un'istruzione SELECT per un report sui contatti può essere scritta:
  `SELECT combo_name FROM cnt WHERE last_name LIKE 'smith%'`

- Il driver ODBC di CA SDM mappa gli attributi come combo_name e gli oggetti come cnt al loro nome DBMS corrispondente.

- Tutta la sicurezza CA SDM, incluse le restrizioni tenancy e di partizione dati, viene applicata automaticamente ai report. Tutte le connessioni tra BusinessObjects e CA SDM sono associate a un contatto CA SDM e ODBC di CA SDM modifica le istruzioni SELECT di input come richiesto al fine di abilitare le restrizioni di protezione associate al ruolo di reporting dell'utente. BusinessObjects non si collega direttamente al database.

- La caratteristica di CA SDM Attribute Alias "appiattisce" o denormalizza il database di CA SDM. Gli alias attributo sono attributi aggiuntivi degli oggetti CA SDM che consentono a una query di fare riferimento agli attributi delle tabelle unite senza un'unione esplicita, consentendo così di usare la tabella di base come una visualizzazione di reporting.
- Il driver ODBC di CA SDM supporta l'espressione letterale della data nelle query, e traduce automaticamente i valori in formato di data interno di CA SDM alla data standard di DBMS.

Importante. Il driver ODBC di CA SDM è supportato soltanto per il reporting di BusinessObjects (Crystal e Web Intelligence). CA SDM non fornisce un client ODBC standalone, e non consiglia l'uso del driver ODBC con applicazioni diverse da BusinessObjects.

Stesura rapporti SQL per BusinessObjects

Tutte le istruzioni SQL utilizzate dai report di BusinessObjects sono elaborate dal driver ODBC di CA SDM. Il driver ODBC supporta le istruzioni SELECT SQL 92 standard con i seguenti cambiamenti ed estensioni:

- I nomi di oggetti CA SDM sono utilizzati al posto dei nomi di tabelle DBMS, e i nomi di attributi di CA SDM sono utilizzati al posto dei nomi di colonne DBMS.
- Un alias nome di CA SDM può essere usato ovunque nella query in cui è valido un nome di colonna. Il driver ODBC sostituisce il riferimento dell'alias attributo con uno o più collegamenti.

  Nota: per ulteriori informazioni, vedere Alias attributi (a pagina 914).
- Gli attributi DERIVED di CA SDM (come combo_name) possono essere usati solo nell'elenco di selezione. Non sono supportati in nessun'altra parte della query, compresa la clausola WHERE.

  Nota: molti oggetti nome combinazione con id utente sono stati forniti nell'universo, come ad esempio l'oggetto nome combinazione cliente con id utente utilizzato come filtro nel report ad hoc di esempio fornito nella *Guida all'amministrazione*. Questi oggetti permettono di utilizzare il nome combinazione come prompt del filtro in query ad hoc con Web Intelligence, per superare la limitazione di includere il nome combinazione nella clausola WHERE. Presentano sia il nome combinazione che l'id utente nel prompt del filtro, ma utilizzano solo gli id utente selezionati nella query SQL risultante.
- Le query possono contenere espressioni di data letterali in uno di questi formati:
  ```
  d'yyyy-mm-dd hh:mm:ss xm' (dove xm può essere am o pm)
  ts'yyyy-mm-dd hh:mm:ss'
  ```
  Queste espressioni possono essere utilizzate ovunque nella query. Il driver ODBC le converte automaticamente al formato di data interno di CA SDM (il numero di secondi dalla mezzanotte del 01 gennaio 1970).

Funzioni PDM

Per contribuire al funzionamento corretto dei tipi di dati e delle funzioni specifiche di CA SDM, il driver ODBC estende l'SQL in modo da supportare varie funzioni di query aggiuntive. Tutte le funzioni supportate dal driver iniziano con la stringa "Pdm", e sono note come funzioni PDM, come si descrive nella tabella seguente:

Funzioni PDM	Descrizione
PdmAddDays([date,] count)	Se utilizzato con un argomento, aggiunge il numero di giorni nell'argomento fino alla data corrente e restituisce il risultato. Se utilizzato con due argomenti, aggiunge il numero di giorni nel secondo argomento al valore della colonna della data specificato nel primo argomento e restituisce il risultato. Questa funzione si può usare ovunque nella query
PdmAddMonths([date,] count)	Se si utilizza con un argomento, aggiunge il numero di mesi nell'argomento fino alla data corrente e restituisce il risultato. Se si utilizza con due argomenti, aggiunge il numero di mesi nel secondo argomento al valore della colonna della data specificato nel primo argomento e restituisce il risultato. Il modulo a un argomento può essere utilizzato in qualsiasi punto nella query. Il modulo a due argomenti può essere utilizzato solo nell'elenco della selezione.
PdmDay([date])	Se utilizzato senza argomenti, restituisce il giorno corrente come numero intero. Se utilizzato con un argomento, restituisce il giorno associato al valore della colonna della data specificato nell'argomento corrispondente. Il modulo privo di argomento può essere utilizzato in qualsiasi punto nella query. Il modulo a un argomento può essere utilizzato solo nell'elenco della selezione.
PdmDownTime(slaName, workshift, startDate, endDate)	Calcola i tempi inattivi tra due date sotto SLA e workshift specificati. Questa funzione può essere utilizzata solo nell'elenco della selezione.
PdmMonth([date])	Se utilizzato senza argomenti, restituisce il mese corrente come numero intero da 1 a 12. Se utilizzato con un argomento, restituisce il mese associato al valore della colonna della data specificato nell'argomento corrispondente. Il modulo privo di argomento può essere utilizzato in qualsiasi punto nella query. Il modulo a un argomento può essere utilizzato solo nell'elenco della selezione.
PdmMonthName([date])	Se utilizzato senza argomenti, restituisce il nome localizzato del mese corrente ("gennaio", "febbraio", ecc). Se utilizzato con un argomento, restituisce il nome localizzato del valore della colonna della data specificato nell'argomento corrispondente. Il modulo privo di argomento può essere utilizzato in qualsiasi punto nella query. Il modulo a un argomento può essere utilizzato solo nell'elenco della selezione.
PdmDay([date])	Se utilizzato senza argomenti, restituisce il giorno corrente come numero intero. Se utilizzato con un argomento, restituisce il giorno associato al valore della colonna della data specificato nell'argomento corrispondente. Il modulo privo di argomento può essere utilizzato in qualsiasi punto nella query. Il modulo a un argomento può essere utilizzato solo nell'elenco della selezione.

Funzioni PDM	Descrizione
PdmSeconds (date)	Restituisce il valore della colonna della data specificato nel relativo argomento calcolato come il numero di secondi dalla mezzanotte del 01 gennaio 1970. Questa funzione può essere utilizzata solo nell'elenco della selezione. Questo argomento è obbligatorio.
PdmString(column)	Restituisce l'equivalente della stringa del valore della colonna specificata nell'argomento. Questa funzione può essere utilizzata con UUID, data, o colonne di stringhe. Questa funzione può essere utilizzata solo nell'elenco della selezione.
PdmToday()	PdmToday() [timeAdj [, day [, month [, year]]]]) Restituisce la data odierna (in secondi a partire da 01/01/70), regolata in base agli argomenti: timeAdj: -1: regola l'ora all'inizio del giorno (0:00:00) +1: regola l'ora alla fine del giorno (23:59:59) day: negativo: regola la data in base al numero di giorni specificato positivo: imposta il giorno sul valore assoluto specificato (o sull'ultimo giorno del mese, a seconda del valore minore) month: negativo: regola la data in base al numero di mesi specificato positivo: imposta il mese sul valore assoluto specificato (o su dicembre (12), a seconda del valore minore) year: negativo: regola la data in base al numero di anni specificato positivo: imposta l'anno sul valore assoluto specificato Le regolazioni vengono applicate secondo l'ordine: anno, mese, giorno. Un argomento zero o omesso viene ignorato.
PdmYear([date])	Se utilizzato senza argomenti, restituisce l'anno corrente come numero intero a quattro cifre. Se utilizzato con un argomento, restituisce l'anno associato al valore della colonna della data specificato nell' argomento corrispondente. Il modulo privo di argomento può essere utilizzato in qualsiasi punto nella query. Il modulo a un argomento può essere utilizzato solo nell'elenco della selezione.

Alias attributi

Gli alias di attributo sono attributi aggiuntivi in oggetti CA SDM che fanno riferimento a dati da tabelle unificate mediante Majic dotted join syntax (in cui la sintassi srelname.attrname è un riferimento all'attributo attrname nella tabella a cui fa riferimento la chiave esterna srelname). Molti alias attributo predefiniti sono forniti in CA SDM Versione 12.9, con nomi che sono in genere identici all'unione Majic corrispondente, con i caratteri di sottolineatura che sostituiscono i punti indicanti l'unione. Per esempio, la seguente istruzione SELECT può essere utilizzata per un report che elenca informazioni circa gli assegnatari della richiesta:

```
SELECT ref_num, assignee_combo_name, assignee_organization_name
   FROM cr WHERE customer_last_name LIKE 'smith%'
```

Il driver ODBC di CA SDM crea automaticamente le unioni necessarie ad accedere alle tabelle a cui fanno riferimento gli alias di attributo. Un utente con il ruolo di amministratore CA SDM può facilmente aggiungere nuovi alias di attributo online, fornendo un modo colonna per colonna di estendere la visualizzazione corrispondente a un oggetto.

Per accedere alla tabella Alias Attributi, selezionare la scheda Administration, e navigare fino a CA SDM, Codes, Attribute Aliases.

pdm_isql Interactive SQL

Un'utilità a linea di comando, pdm_isql, è fornita con CA SDM per permettere l'introduzione interattiva di istruzioni SQL SELECT. Le istruzioni SELECT introdotte in pdm_isql sono inviate al driver ODBC di CA SDM, permettendo di testare le istruzioni SQL SELECT al di fuori di BusinessObjects.

Per utilizzare pdm_isql

1. Verificare che ci sia $NX_ROOT/bin nel percorso.
2. Immettere il comando:

   pdm_isql
3. Nel prompt di pdm_isql immettere il comando seguente:

   connect *nomeutente*password@casd_nomehost*

   (Dove *nomeutente* e *password* sono credenziali di accesso valide di CA SDM, e il nome host è quello di un server CA SDM con motore Web.)
4. Introdurre le istruzioni SQL select seguite da punto e virgola.

Capitolo 21: Creazione di report in CA SDM

Questa sezione contiene i seguenti argomenti:

Generazione rapporti (a pagina 915)
Visualizzazioni di database (a pagina 915)
Impostazione dei metodi di reporting (a pagina 919)
Formattazione dei report (a pagina 919)
Modifica del tipo di ordinamento delle colonne (a pagina 920)
Rapporti riepilogativi e di dettaglio (a pagina 920)
Rapporti di analisi (a pagina 921)

Generazione rapporti

CA SDM fornisce una serie di funzioni e opzioni di reporting incorporate che consentono di effettuare quanto segue:

- Stampare i moduli per asset, singoli Ordini di cambiamento, Issue, Incidenti, Problemi e altro ancora.
- Generare i report riepilogo o dettagli per gli elenchi di Ordini di cambiamento, Issue, Incidenti, Problemi, Richieste, elementi della configurazione.
- Generare report di analisi.

Nota: per ulteriori informazioni su come utilizzare i report di CA SDM, vedere la *Guida in linea*. Oltre ad utilizzare le funzioni di reporting presenti in CA SDM, è possibile creare e generare report personalizzati in base alle tabelle e alle visualizzazioni del database di CA SDM. Per ulteriori informazioni sui report personalizzati, consultare la *Guida all'implementazione.*

Visualizzazioni di database

Il database di CA SDM è un repository per i dati immessi e utilizzati per l'attività del service desk. CA SDM fornisce diverse visualizzazioni di database e consente di creare report personalizzati del database.

Queste visualizzazioni sono di due tipi:

- Visualizzazione di base
- Visualizzazione avanzata

Ulteriori informazioni:

Descrizione dei campi delle visualizzazioni (a pagina 1181)

Visualizzazioni di base

Le visualizzazioni di base si basano sulle tabelle di CA SDM. Queste visualizzazioni mostrano i dati quando l'implementazione utilizza le richieste, gli Incidenti, i Problemi, gli Ordini di cambiamento, le Issue gli asset oppure i contatti/gruppi.

Utilizzando le visualizzazioni di base è possibile progettare e creare molti report, tra cui:

- Elenchi dettagliati e di riepilogo delle Richieste aperte con priorità 1 ordinati per area Richiesta.
- Elenchi dettagliati e di riepilogo degli Ordini di cambiamento assegnati al gruppo di livello 1, aperti per più di 24 ore e ordinati per priorità.
- Numero di Issue aperte per un numero di giorni maggiore di quello specificato, ordinate per priorità, gruppo assegnato o priorità e gruppo assegnato.

Vengono fornite le seguenti visualizzazioni di base:

Nome visualizzazione	Descrizione
View_Contact_Full	Tutti i contatti, inclusi il tipo di contatto, l'ubicazione, le organizzazioni e i tipi di servizio relativi.
View_Contact_to_Environment	Tutti i contatti e il relativo ambiente (asset).
View_Group	Tutti i gruppi definiti nel database.
View_Group_To_Contact	Tutti i contatti (inclusi i responsabili) nelle relative assegnazioni del gruppo.
View_Request	Tutte le richieste, tra cui i tipi di servizio, gravità, urgenze, categorie, asset, numeri di impatto, assegnatari per nome, clienti per nome, gruppi, stati e priorità.
View_Act_Log	Le informazioni sul registro attività richiesta, tra cui il tipo di attività e il nome dell'analista.
View_Request_to_Act_Log	Tutte le richieste con i relativi registri attività. Questa visualizzazione unisce le tabelle View_Request e View_Act_Log.
View_Request_to_Properties	Le richieste e le relative proprietà. Potrebbe non includere tutte le richieste, soprattutto se alle richieste non sono assegnate proprietà.

Nome visualizzazione	Descrizione
View_Change	Tutti gli ordini di cambiamento, tra cui i relativi stati, priorità, categorie, organizzazioni, utenti finali interessati per nome, richiedenti per nome, assegnatari per nome, gruppi, tipi di servizio e numeri di impatto.
View_Change_Act_Log	Le informazioni sul registro attività ordine di cambiamento.
View_Change_to_Change_Act_Log	Tutti gli Ordini di cambiamento con i relativi registri. Questa visualizzazione unisce le tabelle View_Change e View_Change_Act_Log.
View_Change_to_Properties	Gli Ordini di cambiamento e le relative proprietà. Potrebbe non includere tutti gli Ordini di cambiamento, soprattutto se agli Ordini di cambiamento non sono assegnate proprietà.
View_Change_to_Change_WF	Gli Ordini di cambiamento e le relative attività del flusso di lavoro. Potrebbe non includere tutti gli Ordini di cambiamento, soprattutto se agli Ordini di cambiamento non sono assegnate attività del flusso di lavoro.
View_Change_to_Assets	Gli Ordini di cambiamento e i relativi asset. Potrebbe non includere tutti gli Ordini di cambiamento, soprattutto se agli Ordini di cambiamento non sono assegnati asset.
View_Change_to_Requests	Gli Ordini di cambiamento con informazioni di base relative alle Richieste associate. Questa visualizzazione unisce le tabelle View_Change e Call_Request, che potrebbero non includere tutti gli Ordini di cambiamento, soprattutto se gli Ordini di cambiamento non sono associati a Richieste.
View_Issue	Tutte le Issue, con i relativi stati, priorità, categorie, organizzazioni, utenti finali interessati per nome, assegnatari per nome, gruppi, tipi di servizio e così via.
View_Issue_Act_Log	Informazioni sul registro attività Issue.
View_Issue_to_Issue_Act_Log	Tutte le Issue con i relativi registri attività. Questa visualizzazione unisce le tabelle View_Issue e View_Issue_Act_Log.
View_Issue_to_Properties	Le Issue e le relative proprietà. Potrebbe non includere tutte le Issue, soprattutto se non è assegnata alcuna proprietà alle Issue.
View_Issue_to_Issue_WF	Le Issue e le relative attività del flusso di lavoro. Potrebbe non includere tutte le Issue, soprattutto se alle Issue non sono assegnate attività del flusso di lavoro.
View_Issue_to_Assets	Le Issue e i relativi asset. Potrebbe non includere tutti gli asset, soprattutto se alle Issue non sono assegnati asset.

Visualizzazioni avanzate

Le visualizzazioni avanzate si basano sulla tabella audit_log di CA SDM.

Nota: prima di utilizzare queste visualizzazioni è necessario installare le opzioni audit_ins e/o audit_upd in Gestione opzioni e riavviare il sistema.

L'utilizzo delle visualizzazioni avanzate consente di creare report sulla durata di un ticket, ovvero Richiesta, Ordine di cambiamento o Issue, in uno stato specifico. Ad esempio, è possibile creare report per quanto segue:

- Mostrare il tempo trascorso tra l'apertura e l'assegnazione a L2 delle richieste aperte dal primo gennaio 2002.
- Mostrare il tempo in cui le Issue sono rimaste con un livello di priorità 3 prima dell'escalation al livello di priorità 2 per le Issue aperte dal primo gennaio 2002.

Vengono fornite le visualizzazioni avanzate seguenti, ovvero le visualizzazioni della tabella audit_log nel database di CA SDM per l'esecuzione di query specifiche per gli attributi di stato, priorità, gruppo o assegnatario:

Nome visualizzazione	Descrizione
View_Audit_Status	Tutti i ticket ordinati in base al tempo di permanenza in ogni stato. Non include i ticket senza stato.
View_Audit_Priority	Tutti i ticket ordinati in base al tempo di permanenza in ogni priorità.
View_Audit_Group	Tutti i ticket ordinati in base al tempo di permanenza in ogni assegnazione di gruppo. Non include i ticket che non appartengono ad alcun gruppo.
View_Audit_Assignee	Tutti i ticket ordinati in base al tempo di permanenza in ogni singola assegnazione. Non include i ticket senza assegnatario.

Importante. per visualizzare i dati nelle visualizzazioni avanzate è necessario installare le opzioni del registro di audit tramite Gestione opzioni. Per ulteriori informazioni, consultare le descrizioni delle opzioni di audit audit_ins e audit_upd riportate nella Guida in linea.

Ulteriori informazioni:

Utilizzo di Gestione opzioni (a pagina 475)

Impostazione dei metodi di reporting

I metodi di reporting consentono di specificare dove inviare i risultati del report selezionato. Esempi sono i report di riepilogo e dei dettagli disponibili nel menu Report e quelli disponibili nel menu Analisi. Sono forniti diversi metodi di reporting predefiniti, che è anche possibile modificare.

Nota: per informazioni su come definire metodi di report, vedere la *Guida in linea*.

Formattazione dei report

Utilizzando il file dataent.fmt presente in $NX_ROOT/fig/cfg (UNIX) o in directory-installazione\fig\cfg (Windows) è possibile personalizzare vari formati di dati nei rapporti destinati alla stampa. Per visualizzare e modificare questo file, utilizzare un editor di testo. Gli utenti Windows dovrebbero utilizzare WordPad per modificare il file.

Le righe del file seguenti controllano alcuni dei formati di data e ora:

```
default_date = "long_date"
short_date = "M/D/YY// Immettere una data nel formato MM/DD/YY"
long_date = "MM/DD/YYYY// Immettere una data nel formato MM/DD/YY"
default_tod = "hour_12"
hour_12 = "h:mm:ss a(am,pm)// Immettere un orario nel formato hh:mm:ss am/pm"
hour_24 = "HH:mm:ss// Immettere un orario nel formato 00:00:00 - 23:59:59"
hms_12 = "h:mm:ss a(am,pm)// Immettere un orario del giorno nel formato hh:mm:ss am/pm"
hms_24 = "HH:mm:ss// Immettere un orario nel formato 00:00:00 - 23:59:59"
default_date_time = "date_time12"
date_time12 = "DD/M/YYYY h:mm:ss a(am,pm)// Immettere una data e un orario nel formato
DD/MM/YY hh:mm:ss am/pm"
date_time24 = "DD/M/YYYY HH:mm:ss// Immettere una data e un orario nel formato DD/MM/YY
00:00:00-23:59:59"
```

Di seguito è riportato un esempio di come sia possibile modificare queste righe per supportare il formato europeo di data/ora:

```
default_date = "long_date"
short_date = "D/M/YY// Immettere una data nel formato DD/MM/YY"
long_date = "DD/MM/YYYY// Immettere una data nel formato DD/MM/YYYY"
default_tod = "hour_24"
hour_12 = "h:mm:ss a(am,pm)// Immettere un orario nel formato hh:mm:ss am/pm"
hour_24 = "HH:mm:ss// Immettere un orario nel formato 00:00:00 - 23:59:59"
hms_12 = "h:mm:ss a(am,pm)// Immettere un orario del giorno nel formato hh:mm:ss am/pm"
hms_24 = "HH:mm:ss// Immettere un orario nel formato 00:00:00 - 23:59:59"
default_date_time = "date_time24"
date_time12 = "DD/M/YYYY h:mm:ss a(am,pm)// Immettere una data e un orario nel formato DD/MM/YY hh:mm:ss am/pm"
date_time24 = "DD/M/YYYY HH:mm:ss// Immettere una data e un orario nel formato DD/MM/YY 00:00:00-23:59:59"
```

Nota: se si utilizza pdm_extract per esportare i dati dal database di CA SDM a un altro sistema e si desidera estrarre i dati per utilizzare il formato della data specificato nel file dataent.fmt, quando si richiama pdm_extract, utilizzare il flag -d.

Modifica del tipo di ordinamento delle colonne

Gli amministratori possono modificare il tipo di ordinamento delle colonne visualizzate nei report con Web Screen Painter.

Gli utenti possono disporre i dati nei seguenti ordini:

- Crescente (da A a Z, da 0 a 9 o dalla data meno recente a quella più recente)
- Decrescente (a Z ad A, da 9 a 0 o dalla data più recente a quella meno recente).

Nota: per ulteriori informazioni, vedere la *Guida di Web Screen Painter*.

Rapporti riepilogativi e di dettaglio

In CA SDM sono disponibili delle opzioni per segnalazioni di riepilogo e dei dettagli. È possibile selezionare record specifici per un rapporto utilizzando la funzione di ricerca delle finestre di elenco. Ad esempio, nella finestra Dettagli richiesta è possibile immettere i criteri di ricerca per creare un elenco di richieste che è possibile utilizzare in seguito per generare un rapporto.

Per stampare o visualizzare i rapporti di riepilogo e dei dettagli, per prima cosa è necessario selezionare i record da includere nel rapporto. Inoltre, in qualsiasi pagina dei dettagli è possibile stampare una singola pagina del report dei dettagli per ciascun record, selezionando Stampa modulo dal menu File. Per stampare un rapporto per un record appena creato, per prima cosa è necessario salvare il record.

Nota: per ulteriori informazioni sull'uso dei report, vedere la *Guida in linea*.

Rapporti di analisi

La scheda Amministrazione di CA SDM fornisce inoltre i seguenti report di analisi predefiniti, per fornire una visione globale e dettagliata del processo del service desk:

- Richiesta/Issue
- Area Richiesta/Categoria Issue
- Priorità area Richiesta/Priorità categoria Issue

È possibile visualizzare il rapporto di analisi per il giorno corrente, per i trenta giorni precedenti e per l'ultimo anno.

Ulteriori informazioni:

Generazione dei report Richiesta o Issue (a pagina 921)
Generazione dei report Area Richiesta o Categoria Issue (a pagina 922)
Generazione dei rapporti Priorità area Richiesta o Priorità categoria Issue (a pagina 922)

Generazione dei report Richiesta o Issue

I report Richiesta o Issue forniscono dei dati statistici, ad esempio il numero di Richieste o di Issue aperte, il numero di Richieste o di Issue chiuse, il tempo medio di apertura e di chiusura in un periodo specifico. Questo rapporto viene ordinato per data, dalla meno recente alla più recente.

Per generare i report Richiesta o Issue dall'interfaccia Web:

1. Selezionare la scheda Amministrazione.
2. Espandere i nodi Service Desk e Analisi.
3. Selezionare la Richiesta o la Issue.
4. Selezionare il report appropriato in base al periodo di tempo desiderato.

Generazione dei report Area Richiesta o Categoria Issue

I report Area Richiesta o Categoria Issue indicano il numero di Richieste o di Issue aperte nel periodo di tempo specificato per ogni area Richiesta o categoria Issue. Questo rapporto viene ordinato alfabeticamente per area Richiesta o categoria Issue.

Per generare un rapporto Area Richiesta o Categoria Issue dall'interfaccia Web:

1. Selezionare la scheda Amministrazione.
2. Espandere i nodi Service Desk e Analisi.
3. Selezionare la Richiesta o la Issue.
4. Selezionare il report appropriato in base al periodo di tempo desiderato.

Generazione dei rapporti Priorità area Richiesta o Priorità categoria Issue

I rapporti Priorità area Richiesta o Priorità categoria Issue indicano il numero di Richieste o di Issue aperte per priorità nel periodo di tempo specificato per ogni area Richiesta o categoria Issue. Questo rapporto viene ordinato per priorità, dalla più alta alla più bassa e alfabeticamente per area Richiesta o categoria Issue.

Per generare un rapporto Priorità area Richiesta o Categoria Issue dall'interfaccia Web:

1. Selezionare la scheda Amministrazione.
2. Espandere i nodi Service Desk e Analisi.
3. Selezionare la Richiesta o la Issue.
4. Selezionare il report appropriato in base al periodo di tempo desiderato.

Capitolo 22: Gestione della conoscenza

Questa sezione contiene i seguenti argomenti:

Gestione della conoscenza (a pagina 923)
Ricerca di procedure per la gestione della conoscenza (a pagina 924)
Conoscenza e Multi-Tenancy (a pagina 924)
Modalità di impostazione di un archivio della conoscenza (a pagina 925)
Modalità di utilizzo dei documenti dell'archivio della conoscenza (a pagina 928)
Ricerca della conoscenza (a pagina 934)
Chiamata del servlet CAFedSearch attraverso un servizio Web REST (a pagina 935)
Forum (a pagina 936)
Documenti della struttura Knowledge (a pagina 936)
Pianificazione documenti della conoscenza (a pagina 936)
Accesso all'esportazione/importazione (a pagina 946)
Servizi Web (a pagina 962)

Gestione della conoscenza

Per Gestione della conoscenza si intende trovare, organizzare e pubblicare la conoscenza. Gestione della conoscenza acquisisce le informazioni in modo rapido ed efficiente e le trasmette a un utente o gruppo. Le informazioni che vengono acquisite e rese disponibili per il recupero costituiscono il cosiddetto archivio della conoscenza.

Gli utenti possono accedere all'archivio della conoscenza utilizzando un motore di ricerca. Gestione della conoscenza permette agli utenti di creare e gestire contenuto che risiede nell'archivio della conoscenza. È possibile impostare autorizzazioni per le categorie e i documenti per usare gruppi o ruoli. Gestione della conoscenza permette di fornire ai clienti soluzioni per le Issue complesse. Una gestione efficace della conoscenza consente di fornire rapidamente soluzioni ai clienti tramite un processo intuitivo e facile da usare.

Per gestire la conoscenza in modo efficace, effettuare le seguenti operazioni:

- Creare una gerarchia di contenuti significativa
- Identificare le lacune nella conoscenza esistente
- Eseguire aggiornamenti e operazioni di manutenzione per mantenere i contenuti sempre aggiornati
- Misurare il valore del contenuto disponibile

Ulteriori informazioni:

Configurazione di vincoli di partizione dati di Gestione della conoscenza per autorizzazioni in base al ruolo (a pagina 314)

Ricerca di procedure per la gestione della conoscenza

CA SDM fornisce procedure guidate per la gestione della conoscenza, che sono descritte in questa guida e nella *Guida in linea*.

Per ricercare le procedure guidate per la gestione della conoscenza nella *Guida in linea:*

1. Accedere a CA SDM.

   Viene visualizzata la pagina principale CA SDM.

2. Eseguire una qualsiasi delle azioni seguenti:

   - Fare clic su ?, Guida nel menu principale e ricercare Amministrazione, Gestione della conoscenza nella *Guida in linea*.

     Vengono visualizzati gli argomenti relativi alla gestione della conoscenza ed è possibile spostarsi all'interno della gerarchia per ricercare le informazioni desiderate.

   - Fare clic su ?, Guida in linea per la finestra corrente dal menu principale.

     Viene visualizzata la *Guida in linea* con la visualizzazione di un argomento della guida per la pagina per la quale si desiderano informazioni.

Conoscenza e Multi-Tenancy

I documenti della conoscenza e le categorie della conoscenza possono essere specifici per titolare, condivisi tra più titolari o condivisi come pubblici. Quando si ricerca un documento della conoscenza, i risultati visualizzano solo i documenti che possono essere visualizzati dal titolare associato al ticket. I risultati della ricerca FAQ sono specifici per titolare. Le classificazioni dei documenti titolare pubblici devono essere mantenute separate per ciascun titolare.

È possibile amministrare le seguenti impostazioni a livello di titolare:

- Contenuto azione
- Modelli documento
- Processo di approvazione della conoscenza
- Documenti consigliati
- ROI Gestione della conoscenza
- Report

Tutte le altre impostazioni di sistema Gestione della conoscenza sono amministrate globalmente, a livello di fornitore del servizio.

Nota: Multi-Tenancy viene configurata in Gestione opzioni, tramite la scheda Amministrazione.

Modalità di impostazione di un archivio della conoscenza

Per gestire in modo efficiente la conoscenza, non è sufficiente sviluppare un archivio della conoscenza di grandi dimensioni. Gestire la conoscenza comporta infatti anche implementare processi e procedure che consentano di mantenere il contenuto pertinente e accurato.

Per impostare un archivio della conoscenza, effettuare le seguenti operazioni:

1. Determinare come verrà usato l'archivio della conoscenza e il suo ambito di utilizzo
2. Valutare la tipologia di clienti e determinare il tipo di informazioni di cui potrebbero aver bisogno
3. Sviluppare un piano strategico che identifichi le possibili Issue che potrebbero dar luogo a una richiesta di supporto I problemi identificati possono essere usati come guida per determinare quale contenuto deve risiedere nell'archivio della conoscenza
4. Sviluppare l'archivio della conoscenza Creare, organizzare, aggiornare e proteggere tali dati È possibile effettuare tutte queste operazione utilizzando Gestione della conoscenza.

Importazione di dati della conoscenza di esempio

È possibile utilizzare i dati della conoscenza di esempio provenienti da Knowledge Broker, HowTo e Right Answers.

Per usare i dati della conoscenza di esempio, è necessario importare i dati nel database Gestione della conoscenza.

Nota: per maggiori informazioni sui dati di esempio SC, consultare la *Guida all'implementazione*.

Monitoraggio dell'archivio della conoscenza

È possibile controllare l'efficienza dell'archivio della conoscenza utilizzando gli strumenti di reporting descritti di seguito. Questi strumenti consentono di visualizzare statistiche sull'utilità dei documenti e sulla relativa efficacia di risolvere problemi.

Knowledge Report Card

Elenca le statistiche per i documenti creati. Ogni utente ha una scheda report della conoscenza individuale.

Report basati sul Web

Visualizza le metriche che descrivono in che misura la conoscenza soddisfa le esigenze dell'utente. Alcune delle funzionalità più comunemente usate includono:

- Visualizzazione dell'elenco dei documenti consultati più frequentemente
- Visualizzazione delle ricerche utente che non hanno restituito risultati

Reindicizzazione dell'archivio della conoscenza

Se si apportano le seguenti modifiche alle impostazioni di ricerca, è necessario reindicizzare l'archivio della conoscenza utilizzando l'utilità Reindicizzazione della conoscenza:

- Dopo l'importazione di una conoscenza
- Dopo la modifica delle impostazioni di analisi
- Dopo eliminazioni di massa
- In caso di errore nella ricerca

La reindicizzazione è necessaria in quanto i documenti esistenti non riflettono i cambiamenti apportati ai sinonimi, alle parole di disturbo, ai termini speciali e agli altri parametri di ricerca fino a quando non vengono reindicizzati. È necessario reindicizzare tutti i nuovi sinonimi, parole non significative e termini speciali per essere certi che le ricerche di parole chiave nell'archivio della conoscenza siano aggiornate e precise.

Per effettuare questa operazione, è necessario eseguire l'utilità Reindicizzazione della conoscenza da una riga di comando. pdm_k_reindex.exe è il file eseguibile dell'utility Reindicizzazione della conoscenza.

Nota: la reindicizzazione dei documenti dell'archivio della conoscenza può richiedere molto tempo, a seconda delle dimensioni del database. Pertanto, si consiglia di eseguire l'utilità Reindicizzazione della conoscenza solo dopo aver apportato tutte le modifiche.

Indicizzazione e deindicizzazione di impostazioni della coda per l'elaborazione batch e istantanea

Le funzionalità di indicizzazione e deindicizzazione eseguono entrambe un processo batch per includere un numero predefinito di documenti in una sola operazione. Questi processi batch servono per ottimizzare le prestazioni. Più documenti si includono nel batch e migliori saranno le prestazioni del sistema.

Il numero di documenti che è possibile elaborare è limitato. Tale limite dipende dalle dimensioni dei documenti e degli allegati collegati. Le dimensioni del documento vengono calcolate in base al solo testo e ai suo allegati. Gli elementi relativi alle immagini e al formato non vengono inclusi nel calcolo.

Nota: è possibile limitare la dimensione degli allegati utilizzando Libreria allegati, Repository nella scheda Amministrazione e modificando il repository per definire la dimensione limite del file per l'archivio della conoscenza (KB).

Le dimensioni massime consigliate per il batch sono comprese tra 2 e 12 MB (in base al parametro EBR_MAX_INDEX_BATCH_SIZE del file NX.env e alle dimensioni medie del documento).

- Se le dimensioni medie del documento (compresi gli allegati) è circa 0,1 MB, è opportuno mantenere l'impostazione predefinita in NX.env:

  ```
  @EBR_MAX_INDEX_BATCH_SIZE=128
  @NX_EBR_INDEX_QUEUE_TIMEOUT=10
  @NX_EBR_REINDEX_QUEUE_TIMEOUT=1
  @NX_EBR_INDEX_QUEUE_ONLINE=Yes
  @NX_EBR_NON_KD_INDEX_QUEUE_ONLINE=Yes
  ```

  Questa impostazione indica che un batch elabora 128 documenti, che i batch vengono eseguiti ad intervalli di dieci secondi e che, in caso di reindicizzazione, il tempo di attesa tra due batch è un secondo.

- Se le dimensioni medie del documento (compresi gli allegati) è circa 0,5 MB, è opportuno mantenere l'impostazione predefinita in NX.env

  ```
  @EBR_MAX_INDEX_BATCH_SIZE=25
  @NX_EBR_INDEX_QUEUE_TIMEOUT=10
  @NX_EBR_REINDEX_QUEUE_TIMEOUT=10
  @NX_EBR_INDEX_QUEUE_ONLINE=No
  @NX_EBR_NON_KD_INDEX_QUEUE_ONLINE=No
  ```

  Questa impostazione indica che un batch elabora 25 documenti, che i batch vengono eseguiti ad intervalli di dieci secondi e che, in caso di reindicizzazione, il tempo di attesa tra due batch è un secondo.

Modalità di utilizzo dei documenti dell'archivio della conoscenza

I documenti della conoscenza forniscono informazioni sulla conoscenza memorizzata nell'archivio della conoscenza. Per creare una conoscenza di alta qualità è necessario l'intervento di più persone. Ciascun persona avrà il compito di effettuare attività diverse nelle varie fasi del ciclo di vita di un documento della conoscenza. I documenti della conoscenza risiedono nell'archivio della conoscenza e vengono gestiti tramite il seguente processo continuativo:

1. Identificare il contenuto da includere nell'archivio della conoscenza
2. Creare un documento della conoscenza

   I documenti della conoscenza sono collocati in categorie che alcune organizzazioni assegnano ai proprietari.

   Nota: i documenti creati o aggiornati vengono spostati nella cartella Posta in arrivo del proprietario. Finché non vengono pubblicate, le voci della Posta in arrivo potrebbero non apparire come risoluzioni e non venire aggiunte all'archivio della conoscenza.

3. Rivedere il documento

   Quando i documenti arrivano nella cartella Posta in arrivo nel contatore, gli utenti possono eseguire le attività di loro competenza modificando i documenti in base ai propri ruoli.

   Tutti gli utenti con autorizzazioni complete (lettura/scrittura) per il documento possono modificare il documento. Il proprietario corrente ha autorizzazione complete per il documento, ma potrebbe non disporre di autorizzazioni in scrittura esplicite. In caso di problemi con il documento, gli utenti possono creare versioni nuove o effettuare il ripristino ad una versione precedente.

4. Inviare il documento

   La conoscenza può essere inviata dall'interfaccia self-service del cliente o dipendente, ma anche da CA SDM. Questa opzione consente all'analista di inviare una nuova risoluzione utilizzando un ticket esistente. Questa opzione fornisce anche un collegamento tra il problema e la sua risoluzione, e può quindi permettere ad altri utenti con problemi simili di trovare una risoluzione.

5. Pubblicare il documento

   Una volta che un documento è passato attraverso il ciclo del processo di approvazione completo, potrà essere pubblicato. Un documento pubblicato diventa parte dell'archivio della conoscenza visualizzabile alla data di inizio, la quale rappresenta la data corrente in modo predefinito. Il documento è visualizzabile solo per gruppi a cui sono stati concessi diritti di accesso per la lettura. Un utente con autorizzazioni complete può modificare un documento pubblicato.

6. Valutare e decidere quando effettuare le seguenti attività:

   - **Annullamento della pubblicazione del documento—**Il proprietario del documento, un gestore della conoscenza o l'amministratore possono decidere di non pubblicare il documento per scopi di modifica.

   - **Crea versione di rielaborazione—**Gli utenti che dispongono delle autorizzazioni complete di modifica possono creare una versione bozza di rielaborazione di un documento pubblicato mentre rimane in linea, disponibile per la visualizzazione e le ricerche. Una versione di rielaborazione inizia come una copia del documento che è stato sostituito nell'archivio della conoscenza dopo essere stato verificato e ripubblicato.

   - **Ritiro del documento—**Il proprietario del documento, un gestore della conoscenza o un amministratore del sistema possono ritirare il documento dall'archivio della conoscenza.

   Le attività da eseguire e gli utenti che devono eseguire ciascuna attività possono essere impostati in base alla struttura del processo di approvazione esistente nell'organizzazione.

Nota: è possibile tenere traccia delle attività della conoscenza tramite la scheda Registro eventi nelle pagine dei dettagli dei contatti. Ad esempio, se un utente finale visualizza un documento della conoscenza, il registro eventi viene aggiornato e visualizza l'azione eseguita e un collegamento al documento. Il registro eventi tiene traccia anche del periodo di tempo in cui l'utente ha tenuto aperto il documento.

Inoltro conoscenza da CA SDM

Se si acquisisce una conoscenza che si ritiene debba essere aggiunta all'archivio della conoscenza, è possibile inviarla per la valutazione. È possibile inviare la conoscenza sia dall'interfaccia self-service che da CA SDM. Un analista può inviare una nuova risoluzione da un ticket esistente, nel qual caso viene fornito un collegamento tra un problema e la sua risoluzione. Ciò può aiutare altri utenti con problemi simili a trovare una risoluzione. In un'organizzazione in cui ci sono centinaia di ticket aperti contemporaneamente, questa opzione consente di risparmiare tempo prezioso.

È necessario assegnare tutti i documenti della conoscenza a una categoria conoscenza. Se l'area Incidente/Richiesta in CA SDM corrisponde alle categorie conoscenza Gestione della conoscenza, la categoria viene automaticamente selezionata per l'invio della conoscenza.

Invio della conoscenza dalla sezione self-service

Per impostazione predefinita, qualsiasi utente connesso a Gestione della conoscenza può inviare conoscenza per l'analisi utilizzando la pagina Invia conoscenza. Questa pagina permette a un cliente di inviare conoscenza senza dover contattare il rappresentante Service Desk locale. Dopo l'invio, la conoscenza viene inserita in un processo di pubblicazione durante il quale viene esaminata e modificata prima di essere aggiunta all'archivio della conoscenza.

È pertanto importante immettere le informazioni in tutti i campi della pagina Invia conoscenza. Prestare particolare attenzione al completamento del campo Riepilogo. In genere questo campo contiene una breve panoramica del documento che si sta inviando.

Attributi documento

L'impostazione degli attributi documento consente di gestire i documenti nel pool della conoscenza. È possibile aggiornare gli attributi documento per assegnare un nuovo esperto argomento o proprietario al documento. È possibile specificare anche la data in cui il documento sarà disponibile nell'archivio della conoscenza e la sua data di scadenza. Se si selezionano più modelli documento, è possibile modificare l'aspetto di ciascun documento.

Autorizzazioni del documento

È possibile impostare, visualizzare e modificare le autorizzazioni di un documento. Queste autorizzazioni possono essere assegnate a gruppi di persone diverse. Quando si impostano le autorizzazioni, è possibile decidere di ereditare le autorizzazioni dalla categoria principale di documento oppure specificare nuove impostazioni. Per impostazione predefinita, i documenti ereditano le autorizzazioni dalla loro categoria principale. Questa impostazione predefinita gestisce le autorizzazioni di accesso a livello di categoria anziché di documento.

Importante. Quando si crea un documento della conoscenza, accertarsi che le autorizzazioni del documento contengano gli utenti che potrebbero essere assegnati successivamente al documento tramite il processo di approvazione. Quando un gruppo è assegnato a un documento, è possibile che gli utenti appartenenti a tale gruppo non abbiano l'autorizzazione a visualizzare il documento. Se il documento è assegnato a un utente specifico, i vincoli partizione dati predefiniti consentono all'utente di visualizzare il documento.

Modifica della risoluzione

È possibile creare documenti della conoscenza Gestione della conoscenza utilizzando l'editor HTML. Questa funzionalità consente di modificare il campo Risoluzione di un documento della conoscenza e di impostarlo in formato *WYSIWYG (What You See Is What You Get)*. L'utilizzo dell'editor HTML migliora il processo di creazione poiché consente di creare documenti senza che sia necessario immettere il codice HTML, formattare il testo, inserire grafici e tabelle, e creare collegamenti ad altri documenti. Ciò rende il processo di scrittura più veloce e fornisce anche un metodo veloce per modificare un documento a scopo organizzativo.

L'editor HTML consente di effettuare le operazioni seguenti:

- **Visualizzare il codice HTML —**Le schede Modalità progetto e Modalità fonte sulla barra degli strumenti dell'editor HTML permettono di passare da una visualizzazione a un'altra.
- **Formattare il testo—**È possibile digitare il testo del documento direttamente nella finestra dell'editor HMTL. Successivamente, è possibile formattarlo utilizzando le opzioni della barra degli strumenti e dei menu.
- **Inserire grafica—**È possibile inserire grafico nel testo HTML selezionando un'immagine dalla libreria delle immagini oppure caricando della grafica personalizzata.
- **Inserire tabelle—**In un documento della conoscenza è possibile visualizzare una grande quantità di informazioni in modo ordinato. È possibile usare tabelle per formattare queste informazioni in righe e colonne.

- **Inserire collegamenti ipertestuali ad altri documenti—**Quando si crea o modifica un documento della conoscenza è possibile inserire collegamenti ipertestuali ad altri documenti della conoscenza. Ciò consente di collegare un documento della conoscenza ad altri documenti o URL pertinenti. Utilizzando l'editor HTML in modalità Progetto, i collegamenti ipertestuali appaiono come testo sottolineato, di colore blu.
- **Inserire un contenuto azione—**È possibile inserire un contenuto azione (un URL in tempo reale) nel campo Risoluzione di un documento della conoscenza per consentire all'utente di selezionarlo e creare un incidente o eseguire un'altra azione.

Preparazione pubblicazione documento

Dopo aver inviato un documento della conoscenza, è necessario prepararlo per la pubblicazione impostando i relativi attributi e autorizzazioni. L'assegnazione di controlli, come le impostazioni e le categorie, è importante perché permette di organizzare i documenti in modo efficiente.

Ulteriori informazioni:

Modalità di utilizzo dei documenti dell'archivio della conoscenza (a pagina 928)
Attributi documento (a pagina 930)
Autorizzazioni del documento (a pagina 931)

Pubblicazione di documenti

Una volta che un documento è passato attraverso il ciclo del processo di approvazione completo, potrà essere pubblicato. Un documento pubblicato diventa parte dell'archivio della conoscenza visualizzabile alla data di inizio, la quale rappresenta la data corrente in modo predefinito. Il documento è visualizzabile solo per gruppi a cui sono stati concessi diritti di accesso per la lettura.

Quando un documento della conoscenza è pubblicato, in genere l'utente non può modificarlo a meno che non venga prima annullata la pubblicazione. A questo punto è possibile eseguire le modifiche. In questo intervallo di tempo, il documento della conoscenza non è il linea, quindi non è a disposizione degli utenti. Il proprietario del documento, un gestore della conoscenza o un amministratore di sistema può annullare la pubblicazione del documento utilizzando il pulsante Rielaborazione e la casella di controllo Annulla pubblicazione. L'annullamento della pubblicazione di un documento, riporta il documento allo stato di bozza. Un utente amministratore può quindi scegliere la fase successiva del processo del flusso di lavoro.

Controllo delle versioni dei documenti

Utilizzando le funzionalità di controllo delle versioni documento di Gestione della conoscenza, un analista con privilegi di modifica può creare una versione *Bozza di rielaborazione* di un documento. Una versione di rielaborazione inizia come una copia del documento che è stato sostituito nell'archivio della conoscenza dopo essere stato verificato e ripubblicato. Si evita di dover annullare per prima cosa la pubblicazione del documento.

Gli utenti con privilegi di modifica possono anche effettuare le seguenti attività con le versioni:

- Salvare la versione bozza di un documento
- Eseguire il ripristino a una versione precedente di un documento nel caso in cui si verifichi un problema con la versione corrente (Bozza o Pubblicato) Nella scheda Versioni del modulo Aggiorna documento gli utenti possono selezionare diverse versioni per il ripristino finalizzato alla sostituzione della versione corrente.
- Tenere traccia delle versioni dei documenti salvati, eliminati e archiviati nell'archivio della conoscenza

La posta in arrivo dei documenti della conoscenza presente nel contatore CA SDM è il repository per i documenti che si trovano in tutti gli stati, comprese bozze salvate e assegnate e bozze di rielaborazione.

Modalità di gestione delle versioni di documento

Gli amministratori possono effettuare le seguenti operazioni per impostare e gestire versioni di documento:

1. Identificare chi può modificare i documenti pubblicati e creare nuove versioni Rielaborazione - Bozza I privilegi di modifica dipendono dal ruolo usato per i controlli del record di contatto.
2. Definire un modello del processo di approvazione che raggruppi le attività o le fasi da completare durante il ciclo di vita del documento Per impostazione predefinita, un modello di processo di approvazione incorporato consente agli utenti di creare documenti.
3. Specificare se utilizzare il processo di approvazione del documento. Gli analisti a cui è permesso ignorare il processo di approvazione possono identificare le attività con cui desiderano iniziare quando creano una versione Bozza di rielaborazione.
4. Creare regole di archiviazione ed eliminazione per la manutenzione delle versioni dei documenti

Scadenza di documenti

Un documento pubblicato che supera la data di scadenza viene ritirato (vale a dire che il documento viene rimosso dall'archivio della conoscenza e dal processo di approvazione).

Archiviazione ed eliminazione documenti

È possibile gestire le dimensioni del pool della conoscenza utilizzando Archivia ed elimina, che rimuove automaticamente i documenti più vecchi e inutilizzati. La funzionalità Archivia ed elimina migliora l'efficienza delle ricerche della conoscenza perché restituisce solo i documenti correnti.

Questa funzionalità viene eseguita come processo in background e rimuove automaticamente i record inattivi nel database CA SDM in base alle regole configurate dall'utente. Queste regole agiscono sugli oggetti CA SDM ad intervalli di tempo specifici.

Ricerca della conoscenza

Gestione della conoscenza fornisce agli utenti le seguenti opzioni per recuperare la conoscenza:

Esplorazione delle categorie

Consente di trovare soluzioni in base alle categorie. In ciascuna categoria, è possibile impostare ulteriori sottocategorie per limitare il numero di risultati della ricerca a un set di soluzioni che è probabilmente più rilevante per una questione.

Nota: Quando si cercano i documenti della conoscenza tramite la categoria, il risultato della ricerca mostra il numero con la parola chiave utilizzata per la ricerca insieme all'elenco dei documenti. Il numero tra parentesi rappresenta il totale dei documenti nell'archivio della conoscenza che contiene almeno una occorrenza della parola chiave. Ad esempio, durante la ricerca della stringa "assistenza in tempo reale", se 3 documenti contengono ognuno la parola chiave almeno una volta, viene visualizzato "assistenza in tempo reale(3)".

Il numero non viene filtrato secondo i criteri di ricerca specificati. Così, potrebbe non corrispondere al numero di documenti elencati. Inoltre, il numero include solo i documenti elaborati con pdm_k_reindex. Pertanto, i documenti che contengono la stringa specificata ma che sono stati pubblicati dopo il pmd_k_reindex più recente non vengono inclusi nel numero totale.

Per disattivare l'inserimento del numero tra parentesi, aggiungere quanto segue al file $NX_ROOT/NX.env:

```
@EBR_SHOW_WORDS_DF=No
```

Struttura della conoscenza

Pone all'utente una serie di domande per aiutarlo a trovare le possibili soluzioni. Le risposte indirizzano l'utente verso la soluzione che è apparentemente più pertinente.

Segnalibro

Consente di accedere ai documenti visualizzati più frequentemente, che sono inclusi in un elenco di segnalibri.

Chiamata del servlet CAFedSearch attraverso un servizio Web REST

Il servlet CAFedSearch visualizza un'interfaccia RESTful in cui i client di ricerca possono inviare la propria richiesta di ricerca. Questo servlet contiene un adattatore collegabile per consentire ai clienti di integrare i propri motori di ricerca.

L'interfaccia RESTful accetta le richieste HTTP Collection GET mediante il formato OpenSearch.

Procedere come descritto di seguito:

1. Per ottenere una chiave di accesso REST, inviare la richiesta HTTP POST sulla risorsa rest_access con le credenziali di accesso.
2. Per ottenere un token BOPSID mediante la chiave di accesso REST, inviare una richiesta HTTP POST sulla risorsa bopsid. Per ulteriori informazioni, consultare *Metodi dei servizi Web* nella *Guida per l'amministratore*.

   È possibile visualizzare file di esempio anche nella posizione seguente:

   ```
   NX_ROOT\samples\sdk\rest\java
   ```

Utilizzare l'API della ricerca federata per eseguire la ricerca. Inviare la richiesta HTTP GET sulla risorsa di ricerca e trasmettere i criteri di ricerca e il token BOPSID attraverso l'URL di CA SDM. Per ulteriori informazioni, consultare la *Guida all'amministrazione*.

Forum

I forum consentono di fornire informazioni sulle Issues esistenti. I forum permettono la condivisione globale dei documenti o tra gruppi predefiniti che collaborano mettendo a disposizione la conoscenza e raccogliendo idee per affrontare le sfide esistenti.

I forum ampliano il contributo alla conoscenza favorendo la discussione su questioni generali, consigli per la facilità d'uso e così via. È possibile creare un forum utilizzando la scheda Conoscenza o un ticket Service Desk.

Documenti della struttura Knowledge

Progettazione struttura della conoscenza è uno strumento visivo che consente di creare in modo semplice e rapido strutture dalla conoscenza. Una struttura conoscenza è una rappresentazione di conoscenze tecniche relative a un'area specifica. Progettazione struttura della conoscenza consente agli analisti e ai tecnici della conoscenza di creare strutture dettagliate che presentano agli utenti una serie di domande e possibili risposte finché non trovano la risoluzione cercata. Questo strumento elimina script speciali o competenze di programmazione e permette a un qualunque analista che lavori in collaborazione con un esperto dell'argomento di creare una progettazione struttura.

Le strutture della conoscenza possono avere una progettazione complessa. Quindi, è consigliare creare uno schema per associare le progettazione prima di creare la struttura della conoscenza. Lo schema deve contenere una serie di domande, possibili risposte e risoluzioni associate. La gerarchia delle domande e risposte presenti nello schema creato rappresentano la base usata per la creazione della struttura della conoscenza.

Dopo aver effettuato il mapping della struttura della conoscenza, è possibile creare la struttura utilizzando Progettazione struttura della conoscenza.

Pianificazione documenti della conoscenza

La Pianificazione dei documenti della conoscenza fornisce ai gestori dei cambiamenti, ai gestori della conoscenza e agli analisti di livello 2 una visione completa degli eventi principali nel ciclo di vita di gestione della conoscenza. È possibile pianificare gli eventi seguenti per un documento della conoscenza:

- Inoltro
- Pubblicazione
- Revisione
- Scadenza

La scheda Pianificazione gestione della conoscenza visualizza un formato calendario simile a quello della Modifica calendario, ma anziché visualizzare gli orari di avvio e fine, mostra soltanto date specifiche.

La configurazione delle visualizzazioni della pianificazione (a pagina 803) coinvolge l'impostazione di istruzioni macro.

La Pianificazione documento della conoscenza può essere anche esportata nel formato iCalendar.

Nota: quando si esportano pianificazioni in alcuni programmi di calendario, la selezione dell'opzione Apri al posto dell'opzione Salva comporta l'importazione non corretta del file. Per evitare questo problema nelle pianificazioni Gestione della conoscenza e Ordine di cambiamento, selezionare l'opzione Salva anziché Apri. Una volta salvato il file esportato, importarlo attraverso l'interfaccia del programma del calendario.

Filtro pianificazione della conoscenza

Il Filtro pianificazione della conoscenza visualizza i campi seguenti:

Titolare

Filtra la ricerca per titolare. Questo campo mostra l'utente privilegiato in un'installazione multi-tenancy.

Tipo di evento

Filtra la ricerca in base ai tipi di evento seguenti:

- Inoltro
- Revisione
- Pubblicazione
- Ritiro

Pianifica data di inizio

Specifica la data o l'inizio di un intervallo per il filtraggio della cronologia per visualizzare solo le voci di un periodo di tempo specifico.

Pianifica data di fine

Specifica la data per definire la fine di un intervallo per il filtraggio della cronologia per visualizzare solo le voci di un periodo di tempo specifico.

Fuso orario pianificazione

Specifica un fuso orario per visualizzare i risultati della ricerca.

Nota: se non si seleziona alcun fuso orario, gli eventi verranno visualizzati nel fuso orario corrente.

Proprietario

Definisce il nome del contatto assegnato alla gestione del documento. Immettere il nome del contatto nel formato "cognome, nome" o aprire la finestra di dialogo Ricerca Contatto in modo da individuare e selezionare un contatto.

Assegnatario

Definisce il nome del contatto assegnato alla gestione del record. Immettere il nome del contatto nel formato "cognome, nome" o aprire la finestra di dialogo Ricerca Contatto in modo da individuare e selezionare un contatto.

Esperto argomento

Definisce il nome del contatto con esperienza nell'argomento oggetto del documento. Immettere il nome del contatto nel formato "cognome, nome" e aprire la finestra di dialogo Ricerca contatto in modo da individuare e selezionare un contatto.

Stato

Selezionare uno dei seguenti stati di documento per effettuare la ricerca:

- Bozza
- Pubblicato
- Ritirato

Categoria

Definisce il prodotto con cui filtrare i documenti individuati. Immettere il nome della categoria nella casella oppure aprire la finestra Ricerca categoria. Quando si fa clic su Cerca, vengono elencati solo i documenti associati alla categoria specificata.

Visualizzazione iniziale

Selezionare la visualizzazione del Calendario gestione della conoscenza che si preferisce:

Mese

Visualizza un calendario del mese che include la data di inizio implementazione meno recente specificata nel campo Data inizio. Il calendario visualizza informazioni sintetiche su ogni cambiamento compreso nell'intervallo (numero di cambiamento, orari di inizio e fine e il primo elemento della configurazione interessato).

Settimana

Visualizza sette giorni consecutivi in una singola colonna, iniziando dalla data di avvio implementazione meno recente specificata nel campo Data inizio. Il calendario contiene informazioni di riepilogo su ogni cambiamento compreso nell'intervallo specificato (numero di cambiamento, orario di inizio e fine, descrizione di riepilogo, assegnatario, gruppo e i primi dieci elementi della configurazione interessati).

Giorno

Visualizza una visualizzazione simile alla visualizzazione settimanale, eccetto per il fatto che mostra solo il giorno specificato nel campo Data inizio.

***n* giorni**

Mostra una visualizzazione simile a quella della settimana, ad eccezione del fatto che continua per il numero di giorni specificato.

Elenco

Visualizza una pagina di elenco CA SDM standard.

Nota: è possibile fare clic sull'icona Altro per visualizzare il campo Altri argomenti di ricerca. Si consiglia l'uso di questo campo solo da parte di utenti esperti, che conoscono i linguaggi SQL e Majic, per specificare altri argomenti di ricerca non previsti nell'area di ricerca. In questo campo è possibile immettere la clausola SQL WHERE per specificare un argomento di ricerca aggiuntivo.

visualizzazioni della pianificazione della conoscenza

La Pianificazione dei documenti della conoscenza presenta le seguenti visualizzazioni:

Mese

Visualizza il calendario dell'intero mese che comprende la prima data di inizio dell'implementazione specificata nel campo Data di inizio prevista. Il calendario visualizza informazioni sintetiche su ogni cambiamento compreso nell'intervallo (numero di Cambiamento, orari di inizio e fine e il primo elemento della configurazione interessato).

La Pianificazione dei documenti della conoscenza offre funzionalità simili a quelle della visualizzazione mensile degli Ordini di cambiamento, con le seguenti eccezioni:

- Gli eventi della conoscenza presentano soltanto una data (nessun orario) e sono raggruppati secondo il tipo di evento, in maniera simile a quanto avviene per gli Ordini di cambiamento che vengono raggruppati in base ai periodi di tempo e al tipo di Cambiamento.

- I tipi di evento hanno i seguenti colori predefiniti quando si utilizzano le macro schedGroup:
  - Invio—Nero
  - Revisione—Verde
  - Pubblicazione—Blu
  - Ritiro—Rosso

  Nota: una data di revisione riferita al passato indica che probabilmente la revisione non è stata eseguita.

Settimana

Visualizza sette giorni consecutivi in un'unica colonna, partendo dalla prima data di inizio dell'implementazione specificata nel campo Data di inizio prevista. Il calendario contiene informazioni di riepilogo su ogni cambiamento compreso nell'intervallo specificato (numero di cambiamento, orario di inizio e fine, descrizione di riepilogo, assegnatario, gruppo e i primi dieci elementi della configurazione interessati).

Giorno

Visualizza una visualizzazione simile a quella della settimana, ad eccezione del fatto che mostra solo il giorno specificato nel campo Data di inizio prevista.

***n* giorni**

Mostra una visualizzazione simile a quella della settimana, ad eccezione del fatto che continua per il numero di giorni specificato.

Elenco

Visualizza una pagina di elenco CA SDM standard.

Configurazione della visualizzazione di pianificazione

È possibile configurare le visualizzazioni di pianificazione mensili e settimanali specificando le istruzioni pdm_macro nella sezione <head> dei moduli HTMPL che definiscono la pianificazione. Si consiglia l'uso della visualizzazione Origine di Web Screen Painter per modificare questi moduli.

Qualsiasi modulo che visualizzi una pianificazione deve contenere quanto segue:

- Una macro schedConfig
- Almeno una macro schedAttr
- Almeno una macro schedGroup

Le macro di configurazione si trovano in un file fonte a parte, a cui l'istruzione pdm_include fa riferimento nel file fonte principale. Questo file consente di configurare la pianificazione senza modificare il file di origine principale.

Ad esempio, le macro di configurazione per il Modulo calendario cambiamento list_chgsched.htmpl si trovano in un file denominato list_chgsched_config.htmpl. Per la pianificazione relativa al ciclo di vita della conoscenza, è possibile modificare list_kdsched_config.htmpl utilizzando le stesse macro.

list_chgsched_config.htmpl e list_kdsched_config.htmpl si trovano nella seguente directory:

$NX_ROOT\bopcfg\www\htmpl\web\analyst\

Macro schedConfig — programmazione della configurazione

La macro schedConfig specifica che un modulo contiene una pianificazione e fornisce informazioni di configurazione base. I seguenti sono argomenti di macro validi:

autosearch=1|0

Specifica se il modulo di pianificazione ricarica i dati dal server quando l'utente seleziona una visualizzazione al di fuori dell'intervallo date attualmente selezionato. Se si imposta il valore su 1 (valore predefinito), il modulo esegue automaticamente la ricerca quando l'utente seleziona una visualizzazione con uno o più giorni non compresi nell'intervallo di selezione date del filtro di ricerca. Se si imposta il valore su 0, l'utente deve premere il pulsante Cerca per avviare una ricerca.

defaultView=0|1|7|30|99

Specifica la visualizzazione predefinita per il filtro di ricerca come 0 (elenco), 1 (giorno), 7 (settimana), 30 (mese) o 99 (n-giorni).

La specificazione per defaultView interessa solo la visualizzazione iniziale del filtro di ricerca. Una volta visualizzata la pianificazione, CA SDM mantiene automaticamente la selezione di visualizzazione filtro allineata con la visualizzazione corrente.

Impostazione predefinita: 30

firstday=0|1|2|3|4|5|6|7

Specifica il primo giorno della settimana nella visualizzazione mensile come numero compreso tra 0 (domenica) e 6 (sabato).

Impostazione predefinita: 0

export=xxx|0

Specifica il nome di codice del modello utilizzato per l'esportazione nel formato iCalendar. Se si imposta il valore su 0, la funzionalità e il pulsante di esportazione saranno disattivati.

Impostazione predefinita: ChangeSchedule

legend=1|2|0

Specifica la posizione della legenda di pianificazione che mostra il nome e la formattazione dei gruppi nella pianificazione. Impostare il valore su 1 per posizionare la legenda sopra la panificazione, 2 per posizionarla sotto la pianificazione. Impostare il valore su 0 per disattivare la legenda.

Impostazione predefinita: 2

maxGroups=0/*n*

Specifica il numero massimo di gruppi da visualizzare in una sola cella della visualizzazione mensile del calendario.

Se i gruppi pianificati per un solo giorno superano il valore maxGroups, CA SDM visualizza soltanto i primi maxGroups-1, e sostituisce gli ultimi con un collegamento ipertestuale "..altri nn cambiamenti", che consente di visualizzare l'intero elenco al passaggio del mouse o facendo clic. Impostare il valore su 0 per disattivare questa funzionalità e consentire un numero illimitato di eventi in una cella di calendario.

Impostazione predefinita: 4

nday=(n,n,...)

Specifica le selezioni per l'elenco a discesa della visualizzazione n-giorni.

La specificazione è un elenco di conteggi di giorni da includere nell'elenco a discesa, oppure uno 0 per indicare che l'elenco a discesa n-giorni è escluso dalla pianificazione. Il primo valore specificato è l'impostazione predefinita per l'elenco a discesa.

Impostazione predefinita: (3,7,14,28)

round=(*h,min*)|0

Specifica se le date di inizio e di fine pianificazione vengono arrotondate quando si raccolgono ordini di cambiamento o strumenti della conoscenza in gruppi. Specificare round=0 per disattivare l'arrotondamento.

Per impostazione predefinita, oggetti dei gruppi data di inizio e fine pianificazione. Tutte le date di CA SDM includono l'ora e, senza l'arrotondamento, gli oggetti pianificati con anche un solo minuto di differenza si troveranno in gruppi distinti. L'arrotondamento determina il gruppo dopo la modifica dell'ora di inizio a un'ora o un minuto precedenti l'ora di fine a un'ora o un minuto successivi.

Il valore di arrotondamento specifica un'ora o un minuto (ma non entrambi). Le ore vengono arrotondate al multiplo più vicino del valore specificato, ad esempio:

round=(0,15) arrotonda al quarto d'ora più vicino

round=(30) arrotonda alla mezzora più vicina

round=1 arrotonda all'ora più vicina

round=12 arrotonda alla mezza giornata più vicina (00:00 o 12:00)

round=24 arrotonda al giorno più vicino

Impostazione predefinita: (0,15)

timefmt=24hr|([am],[pm])

Specifica il formato degli orari nelle visualizzazioni del calendario della pianificazione.

Il valore predefinito di 24 ore specifica che gli orari vengono visualizzati nel formato a 24 ore (0:01 - 23:59). Il valore alternativo (am,pm) specifica un suffisso per le ore antimeridiane o pomeridiane, oppure per entrambe.

Nota: tutti gli argomenti schedConfig sono opzionali.

Macro schedAttr — specificazione di un attributo archiviato

La macro schedAttr specifica un attributo archiviato per ogni elemento selezionato per l'elenco. Gli attributi archiviati sono disponibili per le informazioni a comparsa nella visualizzazione mensile, per le informazioni dettagliate o di riepilogo negli altri tipi di visualizzazione, e nella funzione JavaScript setSchedEvents(). I seguenti sono argomenti di macro validi:

attr=xxxx

(Obbligatorio) Specifica un attributo dall'oggetto nella pianificazione, come un ordine di cambiamento o un documento della conoscenza. Gli attributi puntati sono ammessi. Nel calendario dei cambiamenti è possibile utilizzare il nome attributo di parola chiave CI*nn* per specificare che i primi elementi della configurazione *nn* associati all'ordine di cambiamento sono inclusi nelle informazioni memorizzate.

Nota: questo è l'unico argomento richiesto per la macro schedAttr.

attrRef=.COMMON_NAME|xxxx

Memorizza l'attributo della tabella di riferimento memorizzata per un attributo SREL (ignorato per gli attributi non-SREL). Il nome dell'attributo specificato deve essere preceduto da un punto.

Impostazione predefinita: .COMMON_NAME

label=

Visualizza un'etichetta per l'attributo nella visualizzazione n-giorni.

Impostazione predefinita: il DISPLAY_NAME Majic dell'attributo

ident=1|0

Specifica se l'attributo è un identificatore per l'oggetto (come un numero di riferimento di un ordine di cambiamento). Gli attributi identificatore vengono visualizzati senza etichetta di fronte al nome del gruppo nelle informazioni a comparsa e nella visualizzazione n-giorni.

Impostazione predefinita: 0

detail=1|0

Specifica se l'attributo è incluso nelle informazioni dettagliate contenute in visualizzazioni diverse da quella mensile. Le informazioni dettagliate sono comprese nelle informazioni visualizzate quando la casella di controllo per la visualizzazione del solo riepilogo non è selezionata.

Impostazione predefinita: 1

hoverInfo=1|0

Specifica se l'attributo è incluso nel popup delle informazioni a comparsa visualizzate nella visualizzazione mensile passando con il mouse su un gruppo o premendo MAIUSC+freccia destra quando il gruppo è selezionato.

Impostazione predefinita: 0

summary=1|0

Specifica se l'attributo è incluso nelle informazioni dettagliate contenute in visualizzazioni diverse da quella mensile. Le informazioni dettagliate sono comprese nelle informazioni visualizzate quando la casella di controllo per la visualizzazione del solo riepilogo non è selezionata.

Impostazione predefinita: 0

Nota: CA SDM visualizza gli attributi in informazioni di riepilogo, dettagliate o a comparsa nello stesso ordine delle rispettive macro schedAttr.

Macro schedGroup — specificazione di un gruppo eventi

La macro schedGroup specifica il nome e il codice colore di un gruppo di elementi. La visualizzazione mensile aggrega tutti gli elementi di un gruppo in un unico evento. Tutte le visualizzazioni eccetto quella mensile mostrano gli elementi individuali nel formato per il gruppo a cui appartengono. I seguenti sono argomenti di macro opzionali:

grpname=xxx

(Obbligatorio) Specifica il nome del gruppo. La macro assegna automaticamente un numero al gruppo e lo assegna a una variabile JavaScript con un nome del modulo schedGroup_xxx, in cui xxx è il nome del gruppo. Questa variabile può essere utilizzata nella funzione JavaScript setSchedEvents() per creare un evento appartenente al gruppo.

Nota: questo è l'unico argomento richiesto per la macro schedGroup.

label=xxx

Specifica un'etichetta per il gruppo. Se specificato, l'etichetta compare in tutte le visualizzazioni.

legend=xxx|0

Visualizza una descrizione del gruppo per la legenda che compare in fondo alla pianificazione. I gruppi compaiono nella legenda se ne esiste almeno un esempio nella visualizzazione corrente. Se si specifica 0 il gruppo sarà sempre escluso dalla legenda.

Impostazione predefinita: 0

color=black|*color*

Specifica il colore del testo negli elementi del gruppo in questione. I colori possono essere specificati in formato CSS; o un colore Web valido o un valore decimale preceduto dal segno del cancelletto.

Esempio: per il rosso immettere "#FF0000" o "red".

Impostazione predefinita: nero

bgcolor=white|*color*

Specifica il colore dello sfondo negli elementi del gruppo in questione. I colori dello sfondo possono essere specificati in formato CSS; o un colore Web valido o un valore decimale preceduto dal segno del cancelletto.

Esempio: per il rosso immettere "#FF000" o "red".

Impostazione predefinita: bianco.

style=normal|bold|italic

Specifica lo stile del testo per il gruppo negli stili normale, grassetto o corsivo.

Impostazione predefinita: normale

La funzione JavaScript setSchedEvents()

La funzione JavaScript setSchedEvents() crea eventi nella pianificazione. Modificare questa funzione per visualizzare nuovi oggetti di gruppo. Gli oggetti di gruppo predefiniti vengono visualizzati per impostazione predefinita.

CA SDM richiama setSchedEvents() una volta per ciascun oggetto (Ordine di cambiamento o documento della conoscenza) selezionato dal filtro di ricerca di pianificazione. La funzione crea eventi per l'oggetto richiamando una seconda funzione, schedEvent(), e trasferendo l'ID di gruppo, la data d'inizio e la data di fine dell'evento.

La funzione può creare un numero illimitato di eventi (compreso zero) per un oggetto. La funzione setSchedEvents() predefinita per il calendario dei Cambiamenti (list_chgsched.htmpl) crea un evento per ogni Ordine di cambiamento e li raggruppa in base al tipo di Cambiamento. Questa funzione è codificata come segue:

```
1.      function setSchedEvents( chg )
2.      {
3.      var grpnum;
4.      switch( chg["chgtype"] - 0 ) {
5.              case 100: grpnum = schedGroup_std;  break;
6.              case 300: grpnum = schedGroup_std;  break;
7.              default:  grpnum = schedGroup_norm; break;
8.      }
9.      chg.schedEvent( grpnum, chg["sched_start_date"], chg["sched_end_date"] );
10.     }
```

Il parametro case specifica l'ID del tipo di cambiamento. Per elencare gli ID caso, consultare Creazione di un tipo di modifica.

La funzione ha un solo argomento di un oggetto JavaScript contenente gli attributi specificati dalle macro schedAttr. L'istruzione switch nelle righe 4-8 esamina l'attributo chgtype dell'Ordine di cambiamento e assegna il numero di gruppo appropriato da una delle variabili schedGroup_xxxx definite da precedenti macro schedGroup. Alla riga 9, richiama la funzione schedEvent() per creare un evento nella pianificazione, passando il numero di gruppo precedentemente assegnato e le date di inizio e fine pianificazione. Le date sono disponibili nell'oggetto argomento perché sono state specificate in precedenti macro schedAttr.

Accesso all'esportazione/importazione

Lo strumento di esportazione/importazione della conoscenza consente di eseguire la migrazione e sincronizzare i dati tra diversi sistemi Gestione della conoscenza e abilita l'esportazione/importazione dei documenti della conoscenza. Utilizzare questo strumento per definire transazioni di importazione/esportazione.

Nota: se Multi-Tenancy è installato, tutte le categorie associate a titolari e pubbliche importate da un sistema precedente vengono visualizzate come pubbliche nel nuovo sistema Multi-Tenancy. Tuttavia, i documenti importati potrebbero essere specifici per titolare.

Per accedere alla pagina KEIT, selezionare Conoscenza, Documenti, Esporta/Importa nella scheda Amministrazione.

Viene visualizzata la pagina Esportazione/importazione che mostra i seguenti elementi:

Esportazione di transazioni

Visualizza un elenco di esportazioni.

Modelli di esportazione/importazione

Visualizza un elenco dei modelli che possono essere modificati.

Importa

Visualizza un elenco di pacchetti disponibili per l'importazione.

Importazione di transazioni

Visualizza un elenco di importazioni.

Nota: quando si importa o esporta conoscenza dall'interfaccia Web, Gestione della conoscenza usa il Ruolo utilità riga di comando predefinito, non il ruolo corrente per il quale l'utente ha eseguito l'accesso a CA SDM. Il ruolo utilità riga di comando predefinito è impostato sul tipo di accesso dell'utente.

Modalità di esportazione/importazione della conoscenza

I modelli di esportazione/importazione consentono di definire una transazione di esportazione/importazione.

Procedere come descritto di seguito:

1. Completare uno dei passaggi seguenti:
   - Creare un modello di esportazione/importazione per creare un pacchetto di esportazione
   - Usare un modello di esportazione/importazione esistente per creare un pacchetto di esportazione
2. Per esportare i dati in un altro sistema, completare uno dei passaggi seguenti:
   - Nella configurazione convenzionale, fare clic su Esporta nella pagina Dettagli del modello di esportazione/importazione.
   - Nella configurazione con disponibilità avanzata, non è possibile esportare i pacchetti dal server applicazioni mediante l'interfaccia Web. Utilizzare l'utilità pdm_ket per esportare i pacchetti dai server.
   - Nella pagina Transizioni di esportazione, fare clic con il pulsante destro del mouse su una transizione e fare clic su Riprova nel menu di scelta rapida.
   - Utilizzo dell'utilità pdm_ket. (a pagina 959)

3. Per Importare i dati della conoscenza dal pacchetto, completare una delle azioni seguenti, a seconda della configurazione di CA SDM:

   - Nella configurazione convenzionale, copiare il pacchetto della conoscenza desiderato dalla directory $NX_ROOT/site/keit/export predefinita e inserirlo nella directory $NX_ROOT/site/keit/import. Nella pagina Elenco Pacchetti di importazione della conoscenza, fare clic con il pulsante destro del mouse su un pacchetto della conoscenza e fare clic su Importa nel menu di scelta rapida.
   - Nella configurazione con disponibilità avanzata, copiare il pacchetto della conoscenza desiderato dalla directory *UNC Shared Location*/export e inserirlo nella directory *UNC Shared Location*/import. Non è possibile importare pacchetti dal server applicazioni mediante l'interfaccia Web, ma con l'utilità pdm_kit è possibile importare i pacchetti da qualsiasi server.
   - Copiare il pacchetto della conoscenza in un'installazione CA SDM mirata e salvarlo nella directory $NX_ROOT/site/keit/import.
   - Nella pagina Elenco Pacchetti di importazione della conoscenza, fare clic con il pulsante destro del mouse su un pacchetto della conoscenza e fare clic su Importa nel menu di scelta rapida.
   - Nella pagina Transizioni di importazione, fare clic con il pulsante destro del mouse su una transizione e fare clic su Riprova nel menu di scelta rapida.
   - Utilizzo dell'utilità pdm_kit_txt (a pagina 960)

Nota: il nome del pacchetto della conoscenza deve iniziare con il prefisso "package_" affinché possa essere incluso nell'elenco della pagina di importazione dei documenti della conoscenza.

Importante. l'utilità di importazione r11,0 è stata rinominata pdm_kit_txt.exe per consentire l'importazione dei fili di testo r11,0. Questa utilità non supporta tutti i miglioramenti al processo di importazione della versione r12.0.

Ulteriori informazioni:

Pacchetti di esportazione/importazione (a pagina 951)

Esportazione di transazioni

È possibile ordinare le transazioni per pacchetto, modello e stato. Tutte le transazioni KEIT vengono registrate nei seguenti file registro:

stdlog

Registra le informazioni di CA SDM.

keitstat.log

Fornisce informazioni statistiche sull'operazione KEIT.

keitinfo.log

Fornisce informazioni dettagliate sull'operazione KEIT.

Nota: in caso di installazione dell'opzione multi-tenancy, la pagina di elenco visualizzerà le impostazioni Titolare e Dati pubblici nel filtro di ricerca. L'opzione Dati pubblici può essere inclusa o esclusa per i dati del titolare: la ricerca viene eseguita unicamente per gli oggetti pubblici. Nelle pagine dei dettagli, selezionare il titolare appropriato dall'elenco. Se si seleziona <vuoto>, l'oggetto è pubblico.

La pagina Transazioni di esportazione contiene i campi elencati di seguito:

Pacchetto

Visualizza il nome del pacchetto di esportazione.

Eseguito da

Visualizza l'utente che ha eseguito l'esportazione.

Ora di avvio

Visualizza l'ora di inizio della transazione.

Ora di fine

Visualizza l'ora di inizio della transazione.

Conteggio documento

Visualizza il numero di documenti esportati.

Conteggio errori

Visualizza il numero di esportazioni con errore.

Avanzamento (%)

Visualizza l'avanzamento della transazione.

Stato

Visualizza lo stato della transazione.

Importazione di transazioni

La pagina Transazioni di importazione consente di ordinare le transazioni per pacchetto, modello e stato facendo clic su una delle colonne.

Nota: in caso di installazione dell'opzione multi-tenancy, la pagina di elenco visualizzerà le impostazioni Titolare e Dati pubblici nel filtro di ricerca. L'opzione Dati pubblici può essere inclusa o esclusa per i dati del titolare: la ricerca viene eseguita unicamente per gli oggetti pubblici. Nelle pagine dei dettagli, selezionare il titolare appropriato dall'elenco. Se si seleziona <vuoto>, l'oggetto è pubblico.

La pagina contiene i campi elencati di seguito:

Pacchetto

Visualizza il nome del pacchetto di importazione.

Eseguito da

Visualizza l'utente che ha eseguito l'importazione.

Ora di avvio

Visualizza l'ora di inizio della transazione.

Ora di fine

Visualizza l'ora di inizio della transazione.

Conteggio documento

Visualizza il numero di documenti importati.

Conteggio errori

Visualizza il numero di importazioni con errore.

Avanzamento (%)

Visualizza l'avanzamento della transazione.

Stato

Visualizza lo stato della transazione.

Ulteriori informazioni:

Visualizza impostazioni di importazione (a pagina 956)

Esportazione/importazione documenti

Per eseguire la migrazione e la sincronizzazione dei dati tra i diversi sistemi Gestione della conoscenza, utilizzare lo strumento KEIT di esportazione/importazione della conoscenza in Amministrazione della conoscenza, che consente di esportare e importare i documenti della conoscenza.

È possibile creare modelli KEIT per definire una transazione di esportazione/importazione.

Nota: per importare i dati della conoscenza r11.0, usare l'utilità pdm_kit-txt.

Pacchetti di esportazione/importazione

Per assegnare i nomi ai pacchetti di esportazione, viene utilizzata la seguente sintassi:

- Nome server
- Data
- Ora di avvio

Nella configurazione convenzionale, è possibile definire directory di pacchetto con l'aggiornamento dell'opzione Percorso file di esportazione/importazione della conoscenza nella pagina Impostazioni generali della scheda Amministratore. Per impostazione predefinita verrà utilizzata la directory $NX_ROOT/site/keit. Riavviare i server di CA SDM (a pagina 49) dopo aver modificato questo percorso.

I pacchetti vengono memorizzati nelle seguenti directory predefinite:

- Pacchetti di esportazione

  $NX_ROOT/site/keit/export
- Importa pacchetti

  $NX_ROOT/site/keit/import

Nella configurazione con disponibilità avanzata, è possibile definire directory di pacchetto con l'aggiornamento dell'opzione Percorso file di esportazione/importazione della conoscenza nella pagina Impostazioni generali della scheda Amministratore. Il percorso deve indicare un'unità condivisa UNC. Riavviare i server di CA SDM (a pagina 49) dopo aver modificato questo percorso. I pacchetti vengono memorizzati nelle seguenti directory:

- Pacchetti di esportazione

  *UNC Shared Location/*export
- Importa pacchetti

  *UNC Shared Location/*import

Per aggiungere attributi alla disponibilità di esportazione/importazione, aggiungere i seguenti nomi di attributi al file NX.env:

@NX_KEIT_AVAILABLE_FIELDS

Aggiunge il nome dell'attributo.

@NX_KET_ADDL_FIELDS

Aggiunge il nome dell'attributo e, se il nuovo attributo è una SREL di un altro oggetto, aggiunge il nome dell'attributo usato per sincronizzare i sistemi di origine e destinazione.

Esempio: aggiunta di attributi

@NX_KEIT_ADDL_FIELDS = STATUS_ID.STATUS,DOC_TEMPLATE_ID.TEMPLATE_NAME

Le directory di esportazione e importazione contengono i seguenti file:

keit_config.xml

Contiene il file di configurazione per un pacchetto di esportazione o importazione.

data.xml

Contiene il file dati con i valori dei documenti della conoscenza.

rep.xml

Contiene i repository citati nel file data.xml.

images

Specifica i file delle immagini incorporati nei documenti della conoscenza.

Visualizzazione di modelli di esportazione/importazione

I modelli di esportazione/importanzione della conoscenza (KEIT) sono utilizzati per definire le transazioni di esportazione/importazione.

Nota: il modello predefinito di esportazione/importazione è chiamato Tutti i documenti e non contiene il campo STATUS_ID. Questo modello crea il file data.xml ed importa i documenti in stato di bozza. Aggiungendo manualmente il campo STATUS_ID al modello Tutti i documenti prima di effettuare l'esportazione, lo stato del documento originale viene conservato dopo l'importazione.

Per visualizzare i modelli Esportazione/Importazione della Conoscenza

1. Fare clic sulla scheda Amministrazione.

   Viene visualizzata la console di amministrazione.

2. Fare clic su Conoscenza, Documenti.

   Fare clic su Esportazione/Importazione, Modelli di esportazione/importazione.

   Viene visualizzato l'Elenco dei modelli di esportazione/importazione della conoscenza.

3. Fare clic su un modello nella colonna Nome.

   Viene aperto l'editor dei modelli KEIT.

Nota: è possibile esportare i risultati sotto forma di elenco in Excel in modo che possano essere usati esternamente a CA SDM facendo clic sul pulsante Esporta nella pagina Elenco.

Ricerca di modelli di esportazione e importazione

Utilizzando la pagina Impostazioni modello di esportazione/importazione della conoscenza, è possibile ricercare un modello.

Nota: se è installata l'opzione multi-tenancy, selezionare il titolare appropriato dall'elenco a discesa. L'opzione pubblica (condivisa) consente di creare l'oggetto per tutti i titolari. Viene visualizzato un elenco a discesa dei titolari nel filtro della ricerca. Se si seleziona <vuoto> in questo elenco a discesa, la ricerca è pubblica. Nella pagina elenco è visualizzata anche una colonna relativa al titolare.

Per effettuare la ricerca dei modelli di Esportazione/Importazione della Conoscenza

1. Dalla scheda Amministrazione, accedere a Conoscenza, Documenti, Esportazione/Importazione, Modelli di esportazione/importazione.

   Viene visualizzato l'Elenco dei modelli di esportazione/importazione della conoscenza.

2. Fare clic su Cerca ed inserire i parametri di ricerca.

   Vengono visualizzati i risultati della ricerca.

3. Fare clic su Mostra filtro.

   Viene visualizzato il filtro.

4. Modificare la ricerca utilizzando le opzioni seguenti:

   Pacchetto

   Ricerca per nome pacchetto.

   Data prima modifica

   Effettua la ricerca per la data di modifica meno recente.

   Data ultima modifica

   Effettua la ricerca per la data di modifica più recente.

   Altri argomenti di ricerca

   Offre argomenti di ricerca aggiuntivi.

   Vengono visualizzati i risultati della ricerca.

5. Fare clic su un modello nei risultati della ricerca.

   Viene aperto il modello.

Creazione di un modello di esportazione/importazione

È anche possibile creare e modificare un modello utilizzando la pagina Impostazioni modello di esportazione/importazione della conoscenza nella scheda Amministrazione.

Per creare un modello di Esportazione/Importazione della conoscenza

1. Dalla scheda Amministrazione, accedere a Conoscenza, Documenti, Esportazione/Importazione, Modelli di esportazione/importazione.

   Viene visualizzato l'Elenco dei modelli di esportazione/importazione della conoscenza.

2. Fare clic su Crea Nuovo.

   Viene visualizzata la pagina Crea nuovo modello esportazione/importazione.

3. Inserire i dati nei seguenti campi:

   Nome modello

   Identifica il nome del modello.

   Descrizione

   Fornisce una breve descrizione del modello.

4. Completare i campi appropriati nelle tabelle seguenti:

   - Esportazione di campi (a pagina 955)
   - Esportazione del filtro (a pagina 955)
   - Importazione delle impostazioni (a pagina 956)

   Fare clic su Salva.

   Il modello è stato creato.

Ulteriori informazioni:

Esportazione di transazioni (a pagina 948)
Importazione di transazioni (a pagina 949)

Visualizzazione dei campi di esportazione

Per visualizzare i campi di esportazione, è necessario creare un modello di esportazione/importazione della conoscenza (KEIT).

Viene visualizzata la scheda Esporta campi che include i seguenti campi:

Disponibile

Visualizza i campi del documento della conoscenza che possono essere esportati.

Nota: per mantenere lo stato dei documenti, come Bozza, durante il processo di esportazione e importazione, aggiungere STATUS_ID alla colonna Esportato.

Esportato

Specifica i campi del documento da esportare.

Esporta allegati

Esporta gli allegati dei file del documento della conoscenza.

È possibile usare i tasti freccia nella sezione Seleziona attributi documento per aggiungere gli attributi del documento da esportare.

Nota: se si modifica il modello di esportazione/importazione con Firefox, le dimensioni dell'elenco non cambiano quando si utilizzano i tasti freccia durante la prima modifica. Tuttavia, se si chiude e si riapre il documento in modalità di modifica e si utilizzano nuovamente i tasti freccia, le dimensioni dell'elenco vengono modificate. Ciò non si verifica quando si utilizza Internet Explorer.

Importante I campi esportati nel modello KEIT hanno una priorità più alta se sono stati selezionati come predefiniti nella scheda Importa impostazioni. Se si seleziona un campo di esportazione predefinito nella scheda Importa impostazioni, questo non viene elaborato come campo predefinito.

Visualizzazione del filtro di esportazione

Per visualizzare il filtro di esportazione, è necessario creare un modello di esportazione/importazione della conoscenza (KEIT).

Viene visualizzata la scheda Esporta filtro che include i seguenti campi:

Categoria

Apre la pagina Categoria della conoscenza. È possibile usare questa opzione per aggiungere categorie all'elenco della scheda Esporta filtro.

Rimuovi categoria

Rimuove le categorie dall'elenco della scheda Esporta filtro.

Cancella categoria

Cancella l'elenco delle categorie nella scheda Esporta filtro.

Includi categorie figlio

Esporta i documenti dalle categorie figlio delle categorie esportate.

Includi categorie secondarie

Esporta le categorie secondarie dei documenti esportati.

Includi tutti i documenti collegati alle categorie selezionate

Esporta tutti i documenti collegati alle categorie selezionate.

Nota: questa opzione è abilitata solo se si seleziona Includi categorie secondarie.

Filtro addizionale

Specifica una clausola WHERE aggiuntiva.

Visualizza impostazioni di importazione

Per visualizzare le impostazioni di importazione, creare un Modello di esportazione/importazione della conoscenza (KEIT).

Viene visualizzata la scheda Importa impostazioni la quale contiene i campi seguenti:

Soglia di errore (%)

Termina il processo di importazione (imposta lo stato su Errore) se la percentuale di errori eccede il numero specificato.

Sovrascrivi documenti pubblicati

Consente ai documenti importati di sovrascrivere i documenti pubblicati del server di CA SDM.

Sovrascrivi documenti in stato non pubblicato

Consente ai documenti importati di sovrascrivere i documenti non pubblicati del server di CA SDM.

Utilizza valori predefiniti durante la sovrascrittura dei documenti

Utilizza i valori predefiniti sui documenti sovrascritti per i campi definiti.

Indicizza documenti immediatamente

Indicizza il documento dopo il processo di importazione.

Stato

Selezionare Bozza, Pubblicato o Ritirato.

Priorità

Imposta il livello di priorità delle impostazioni di importazione.

Modello

Seleziona uno dei seguenti modelli predefiniti:

- Incorporato - Documento della conoscenza
- Incorporato - Struttura della conoscenza
- Incorporato - Modifica rapida

Proprietario

Consente di impostare il proprietario aprendo la pagina Ricerca contatto.

Autore

Consente di impostare l'autore aprendo la pagina Ricerca contatto.

Esperto argomento

Consente di impostare l'esperto argomento aprendo la pagina Ricerca contatto.

Assegnatario

Consente di impostare l'assegnatario aprendo la pagina Ricerca contatto.

Data scadenza

Apre l'assistente data.

Data revisione

Apre l'assistente data.

ID prodotto

Consente di impostare l'ID prodotto aprendo la pagina Ricerca prodotto.

Asset

Consente di aprire la pagina Ricerca elemento della configurazione.

Causa principale

Apre la pagina Ricerca causa principale.

Priorità Service Desk

Imposta la priorità del Service Desk delle impostazioni di importazione.

Gravità

Imposta il livello di gravità delle impostazioni di importazione.

Impact

Imposta il livello di impatto delle impostazioni di importazione.

Urgenza

Imposta il livello di urgenza delle impostazioni di importazione.

Modifica di un modello di esportazione/importazione

È possibile modificare i modelli di esportazione e importazione tramite la pagina Elenco Modelli di esportazione/importazione della conoscenza.

Per modificare un modello di esportazione o importazione:

1. Selezionare Conoscenza, Documenti, Esportazione/Importazione, Modelli di esportazione/importazione.

   Viene visualizzato l'Elenco dei modelli di esportazione/importazione della conoscenza.

2. Selezionare un modello.

   Viene visualizzata la pagina Dettagli modello.

3. Fare clic su Modifica.

   Modificare i campi appropriati:

   Nome modello

   Identifica il nome del modello.

   Descrizione

   Fornisce una breve descrizione del modello.

4. Modificare i campi appropriati nelle seguenti schede:

   - Esportazione di campi (a pagina 955)
   - Esportazione del filtro (a pagina 955)
   - Importazione delle impostazioni (a pagina 956)

5. Fare clic su Salva.

   Le modifiche vengono salvate.

Ulteriori informazioni:

Importazione di transazioni (a pagina 949)

Utilità pdm_ket—Strumento di esportazione della conoscenza

L'utilità pdm_ket consente di esportare la conoscenza utilizzando un modello creato tramite l'interfaccia Web da un computer di origine a un pacchetto della conoscenza.

Durante l'esportazione, gli allegati e i relativi collegamenti vengono esportati nel file data.xml. Prima di importare gli allegati, è necessario spostarli manualmente nella seguente directory sul server in background:

$NX_ROOT/site/attachments/default

Nota: Per la configurazione con disponibilità avanzata, è possibile eseguire l'utilità pdm_ket tramite il percorso UNC degli allegati.

È possibile utilizzare questa utilità per:

- Creare un file di configurazione basato sul modello di esportazione della conoscenza correlato
- Esportare i dati con l'UUID del documento e contenuto come il titolo, il riepilogo, il problema, la risoluzione e altri attributi del documento come il proprietario, lo stato e così via
- Esportare tutte le immagini univoche usate dai documenti esportati (che vengono sempre esportate)
- Esportare tutti gli allegati univoci usati dai documenti esportati (campo EXP_ATTMNT)

  I file vengono copiati dal repository remoto nella cartella del pacchetto locale.

L'utilità viene richiamata nel modo seguente:

```
pdm_ket -n <nome modello> [-h] ]-v]
```

-n <nome modello>

Specifica il nome del modello usato per l'esportazione (distingue tra lettere minuscole e maiuscole).

-h

(Opzionale) Visualizza la Guida in linea dell'utilità.

-v

(Opzionale) Consente la registrazione estensiva (bop_logging) di eventi di programma. Questa opzione viene comunemente utilizzata per la risoluzione dei problemi interni.

Esempio: utilizzo di pdm_ket per esportare la conoscenza tramite il modello my_template

```
pdm_ket -n my_template
```

È possibile pianificare l'esecuzione dell'utilità pdm_ket utilizzando un'utilità di pianificazione di terze parti per l'esportazione dei documenti della conoscenza.

Utilità pdm_kit—Strumento di importazione della conoscenza

L'utilità pdm_kit importa i dati sul server di destinazione in base alle impostazioni contenute nel file di configurazione di un pacchetto.

Importante. Prima di eseguire l'utilità pdm_kit dal server applicazioni, accertarsi che il server in background possa accedere al percorso (locale o UNC) del pacchetto. Se il server in background non è in grado di accedere a questo percorso, il pacchetto non viene importato dal server applicazioni.
Importante. L'utilità di importazione r11.0 è stata rinominata pdm_kit_txt.exe per consentire l'importazione dei file di testo r11.0. Questa utilità non supporta tutti i miglioramenti al processo di importazione della versione Versione 12.9.

I dati citati in precedenza dall'utilità pdm_ket acquisiscono l'UUID reale o il valore ID del server di destinazione. Quando si esegue l'utilità pdm_kit viene applicato un nuovo parametro id utente. Il funzionamento dell'utilità pdm_kit è il seguente:

1. Importa i documenti sostituendo il valore id utente (per i contatti) o il nome citato (per i campi come l'asset) con l'UUID appropriato del server di destinazione.
2. Importa le immagini.
3. Importa gli allegati.
4. Carica i file dalla cartella del pacchetto locale nei repository remoti.

Nota: se l'opzione di modifica dei documenti pubblicati è disabilitata, il documento importato viene creato come versione di rielaborazione.

L'utilità viene richiamata nel modo seguente:

```
pdm_kit [-h] -f -u [-v]
```

-h

(Opzionale) Visualizza la Guida in linea dell'utilità sull'interfaccia.

-f

Specifica il percorso del pacchetto.

-u

Specifica l'utente predefinito.

-v

(Opzionale) Consente la registrazione estensiva (bop_logging) di eventi di programma. Questa opzione viene comunemente utilizzata per la risoluzione dei problemi interni.

Nota: Per la configurazione con disponibilità avanzata, è possibile eseguire l'utilità pdm_kit sul server in background. Per Windows, è anche possibile eseguire l'utilità pdm_kit sul server applicazioni se il pacchetto risiede in un'unità condivisa UNC. Per piattaforma non Windows, non è possibile eseguire utilità pdm_kit sul server applicazioni.

Esempio: uso di pdm_kit per l'importazione di un pacchetto

```
pdm_kit -f c:\package_path -u ServiceDesk
```

Consentire agli utenti di esportare e importare conoscenza

È possibile permettere agli analisti di concedere autorizzazioni di esportazione e importazione gestendo l'elenco dei ruoli nella scheda Amministrazione.

Per concedere autorizzazioni di esportazione/importazione:

1. Accedere a Gestione ruoli e protezione, Gestione ruoli, Elenco ruoli.

   Viene visualizzato l'Elenco ruoli.

2. Selezionare un ruolo con il tipo di interfaccia Analista.

   Viene visualizzata la pagina Dettagli ruolo.

3. Fare clic su Modifica.

   Viene visualizzata la pagina Aggiorna ruolo.

4. Fare clic sulla scheda Conoscenza.

   Effettuare una delle operazioni seguenti:

   - Selezionare la casella di controllo Consenti esportazione.
   - Selezionare la casella di controllo Consenti importazione.
   - Selezionare entrambe le caselle di controllo.

5. Fare clic su Salva.

   Viene nuovamente visualizzata la pagina Dettagli ruolo.

6. Riesaminare i cambiamenti nella scheda Conoscenza.

   Chiudere la pagina Dettagli ruolo.

È possibile anche impedire agli utenti l'esportazione/l'importazione deselezionando le caselle di controllo nella scheda Conoscenza della pagina Dettagli ruolo.

Servizi Web

È possibile accedere alla conoscenza tramite i servizi Web SOAP. Sono disponibili vari metodi che consentono la ricerca, il recupero, la creazione e l'aggiornamento di documenti, nonché una serie di altre operazioni.

Nota: per maggiori informazioni sui servizi Web SOAP, consultare la *Guida all'implementazione*.

Capitolo 23: Amministrazione Gestione della conoscenza

Questa sezione contiene i seguenti argomenti:

Amministrazione della conoscenza (a pagina 963)
Ricerca di procedure per l'amministrazione della conoscenza (a pagina 963)
Ruoli e funzioni Gestione della conoscenza (a pagina 964)
Come gestire i privilegi dei ruoli e la visibilità dei documenti (a pagina 975)
Contenuto azione (a pagina 975)
Processo di approvazione dei documenti (a pagina 981)
Policy automatiche (a pagina 988)
Controllo del documento della conoscenza (a pagina 993)
Impostazioni di sistema di Gestione della conoscenza (a pagina 1050)

Amministrazione della conoscenza

È possibile configurare le impostazioni amministrative per Gestione della conoscenza. È possibile impostare opzioni della conoscenza self-service (a pagina 966) che soddisfino le esigenze degli utenti e creare così un ambiente efficace e produttivo per gestire e fornire la conoscenza. Utilizzare la scheda Amministrazione per impostare le opzioni di sistema. È possibile impostare autorizzazioni della conoscenza in base al gruppo o al ruolo di un contatto. Ciò consente di applicare impostazioni per confermare la funzionalità e l'uso di Gestione della conoscenza.

Importante La reindicizzazione dei documenti nell'archivio della conoscenza e l'esecuzione del calcolo per le norme automatiche e la scheda Report della conoscenza possono richiedere molto tempo. Pertanto, è consigliabile effettuare queste operazioni al di fuori dell'orario di lavoro o quando il sistema è meno occupato.

Ricerca di procedure per l'amministrazione della conoscenza

CA SDM fornisce procedure guidate per la gestione della conoscenza, che sono descritte in questa guida e nella *Guida in linea*.

Per ricercare le procedure guidate per l'amministrazione della conoscenza nella *Guida in linea:*

1. Accedere a CA SDM.

   Viene visualizzata la pagina principale CA SDM.

2. Eseguire una qualsiasi delle azioni seguenti:
   - Fare clic su ?, Guida nel menu principale e ricercare Amministrazione, Amministrazione della conoscenza nella *Guida in linea*.

     Vengono visualizzati gli argomenti relativi all'amministrazione della conoscenza ed è possibile spostarsi all'interno della gerarchia per ricercare le informazioni desiderate.
   - Fare clic su ?, Guida in linea per la finestra corrente dal menu principale.

     Viene visualizzata la *Guida in linea* con la visualizzazione di un argomento della guida per la pagina per la quale si desiderano informazioni.

Ruoli e funzioni Gestione della conoscenza

Gestione della conoscenza è stato progettato per un'ampia gamma di utenti, dagli amministratori di sistema e i gestori della conoscenza, che si occupano della manutenzione del prodotto, fino ai clienti e ai dipendenti, che utilizzano il sistema per trovare soluzioni ai loro problemi. Benché possano essere assegnati più ruoli a un utente, i ruoli utente di base disponibili in Gestione della conoscenza sono i seguenti:

- **Cliente—**Utente finale esterno che esegue attività self-service di base.
- **Dipendente—**Utente finale interno che esegue attività self-service di base.
- **Analista della conoscenza—**Utente responsabile di una o più fasi del processo di gestione della conoscenza. Questo utente interagisce con gli analisti Service Desk per creare e mantenere una base della soluzione di qualità.
- **Gestione della conoscenza—**Supervisore per l'analista della conoscenza. Questo ruolo si occupa di riassegnazioni ed escalation di documenti della conoscenza e gestisce, giorno per giorno gli aspetti amministrativi delle soluzioni, inclusi la creazione della struttura di categoria, definendo il processo di approvazione, gestendo parole non significative, termini speciali, sinonimi e opzioni che sono più dinamiche in natura di quanto lo siano i controlli di amministrazione della gestione della conoscenza.
- **Amministratore—**Si tratta di un amministratore che accede a tutte le funzionalità dei prodotti CA SDM e Gestione della conoscenza con un singolo ruolo. Questo ruolo è normalmente utilizzato durante l'implementazione di CA SDM per assicurare che tutti gli utenti e i ruoli siano impostati correttamente così come un ambiente CA SDM con un utente singolo che esegue tutte le attività di amministrazione.
- **Amministratore della gestione della conoscenza—**Amministratore responsabile della configurazione e del monitoraggio del processo di gestione della conoscenza. Questo ruolo si occupa anche di creare la struttura di categoria, definire il processo di approvazione e configurare le impostazioni di ricerca e protezione predefinite.

Nell'ambiente CA SDM ciascun ruolo è associato a livelli di accesso diversi. Questi livelli consentono di definire le attività che possono essere eseguite da ciascun ruolo.

Ulteriori informazioni:

Interfacce utente di Gestione della conoscenza (a pagina 965)
Funzioni di gestione e configurazione Gestione della conoscenza (a pagina 965)
Opzioni della conoscenza self-service (a pagina 966)
Documenti e utenti (a pagina 972)
Come gestire i privilegi dei ruoli e la visibilità dei documenti (a pagina 975)

Interfacce utente di Gestione della conoscenza

È possibile usare le seguenti interfacce utente per gestire la conoscenza:

- **Self-service—**Tramite l'interfaccia self-service, i clienti e i dipendenti che utilizzano CA SDM possono accedere ai documenti della conoscenza e inviare conoscenza per ulteriori valutazioni. I clienti possono effettuare ricerche, sfogliare o utilizzare segnalibri per individuare e visualizzare documenti della conoscenza.
- **Documenti della conoscenza --** Nell'interfaccia documenti della conoscenza, a cui si accede dal nodo Documenti della conoscenza presente nel contatore CA SDM, tutti gli utenti del sistema possono visualizzare la cartella della posta in arrivo e i commenti di completamento. L'*amministratore* gestisce i propri documenti non assegnati/non indicizzati, le policy di durata del documento automatizzati e i forum degli utenti.
- **Gestione della conoscenza—**Nell'interfaccia di gestione della conoscenza, a cui è possibile accedere tramite la scheda Conoscenza in CA SDM, l'*analista della conoscenza* o il *gestore della conoscenza* possono ricercare, organizzare e pubblicare la conoscenza. Possono inoltre filtrare i documenti visualizzati applicando opzioni avanzate, e ordinare i risultati per pertinenza, data di modifica e altro ancora.
- **Amministrazione della conoscenza --** Nell'interfaccia di amministrazione della conoscenza, a cui si accede tramite il nodo Conoscenza nella scheda Amministrazione CA SDM, l'*amministratore, il gestore della conoscenza o l'amministratore della gestione conoscenza* possono impostare numerosi opzioni di sistema. Le impostazioni aiutano a rendere più conformi il funzionamento e l'uso di Gestione della conoscenza.

Funzioni di gestione e configurazione Gestione della conoscenza

È possibile effettuare le seguenti funzioni di configurazione e gestione in Gestione della conoscenza:

- Creare "un'azione contenuto" (un URL di un'azione in tempo reale) da inserire nel campo Risoluzione di un documento
- Impostare il processo di approvazione e definire il processo relativo al ciclo di vita del documento della conoscenza

- Impostare policy automatiche per automatizzare determinate attività nel processo di approvazione dei documenti della conoscenza
- Configurare le opzioni del documento relative ai commenti, all'invio della conoscenza, ai modelli e alle impostazioni del documento
- Creare i modelli che specificano la modalità di visualizzazione di un documento
- Gestire il motore di ricerca Gestione della conoscenza predefinito e configurare le parole non significative, i termini speciali e i sinonimi utilizzati per eseguire le ricerche per parole chiave e in linguaggio naturale
- Creare i "documenti consigliati" che vengono visualizzati nell'interfaccia self-service quando gli utenti ricercano soluzioni della conoscenza
- Gestire la struttura della categoria conoscenza per facilitare l'accesso ai documenti
- Impostare la Scheda report della conoscenza e le impostazioni di sistema generali
- Definire indagini per raccogliere e analizzare il feedback dei clienti sulle prestazioni del documento della conoscenza
- Gestire l'integrazione di Gestione della conoscenza con CA SDM, incluso il mapping dei campi e la configurazione della ricerca di richieste e questioni

Opzioni della conoscenza self-service

I clienti e i dipendenti che utilizzano CA SDM possono accedere ai documenti della conoscenza tramite l'interfaccia self-service. I clienti possono effettuare ricerche, sfogliare o utilizzare segnalibri per individuare e visualizzare documenti della conoscenza. Permettere ai clienti di accedere ai documenti della conoscenza e ai servizi significa permettere loro di trovare direttamente le risposte e di sovraccaricare meno le risorse.

Nell'interfaccia utente self-service, i dipendenti e i clienti possono visualizzare le seguenti opzioni di soluzione della conoscenza:

- **Cerca soluzioni della conoscenza --**I dipendenti e i clienti possono immettere parole chiave e frasi in un campo di ricerca per recuperare un elenco di soluzioni della conoscenza. È possibile configurare questa opzione nella seguente ubicazione: Amministrazione, Conoscenza, Cerca, Impostazioni di ricerca.
- **Visualizza soluzioni principali—**I dipendenti e i clienti possono visualizzare un elenco delle soluzioni principali nell'interfaccia self-service. La seguente impostazione Amministratore: Amministrazione, Conoscenza, Sistema, Impostazioni generali, Soluzioni principali - Numero di documenti da visualizzare determina il numero di documenti che possono essere visualizzat**i**.

- **Prompt per indagine della conoscenza**-- Dopo aver aperto un documento della conoscenza, l'utente può leggere il documento e accedere a una serie di domande dell'indagine. Una di queste domande permette al cliente di indicare tramite un prompt se ritiene che il problema sia stato risolto. È possibile configurare questa opzione nella seguente ubicazione: Amministrazione, Conoscenza, Indagine soluzione, Impostazioni di ricerca.
- **Suggerisci conoscenza—**I dipendenti e i clienti possono, laddove permesso, visualizzare un elenco di consigli della conoscenza quando creano un ticket nell'interfaccia self-service. È possibile configurare questa opzione nella seguente ubicazione: Amministrazione, Conoscenza, Integrazione Service Desk, Suggerisci conoscenza.

Ricerca avanzata

Nelle impostazioni Ricerca avanzata, i clienti e i dipendenti possono usare le seguenti opzioni per ottimizzare la ricerca di una soluzione a un problema:

Ricerca Gestione della conoscenza

Ricerca alcune parole chiave specifiche, che vengono usate come corrispondenze preliminari.

Ricerca in linguaggio naturale

Ricerca parole e account in base alla vicinanza delle parole, l'ordine della parola e la rilevanza.

I risultati della ricerca vengono elencati in ordine di rilevanza. La pertinenza viene definita in base ai criteri di ricerca specificati (espressa come Eccellente, Buono, ecc). I documenti con maggiore pertinenza (ECCELLENTE) vengono elencati per primi.

Ciascun risultato può includere un titolo, visualizzato sotto forma di collegamento, un riepilogo del documento e ulteriori statistiche relative al documento, come la classificazione della rilevanza, l'ID del documento, la data di modifica, la classificazione FAQ e il numero di accessi.

A seconda di come l'amministratore del sistema ha configurato Gestione della conoscenza, gli utenti possono aprire un incidente, classificare un documento e fornire commenti quando un documento della conoscenza è aperto.

Informazioni sui documenti della conoscenza

Ciascun documento della conoscenza contiene campi documento chiave che forniscono informazioni. A seconda del modello documento usato, è possibile che i campi visualizzati o il loro aspetto siano diversi nel documento.

Ciascun documento è identificato da un titolo. Il documento include anche le seguenti informazioni:

Riepilogo

Fornisce un riepilogo del documento e una breve descrizione del problema.

Problema

Descrizione del problema.

Risoluzione

Spiega come risolvere il problema sotto forma di testo o in formato HMTL.

Vedi anche

Elenca i documenti correlati al documento corrente. Se si seleziona un collegamento ipertestuali, si apre una nuova pagina che contiene il documento.

Allegati

Elenca tutti i file allegati al documento e che è possibile scaricare. Gli allegati forniscono ulteriori informazioni sul documento.

Categorie correlate

Elenca le categorie correlate al documento corrente. Se si seleziona il collegamento ipertestuale di una categoria, la pagina Strumenti ricerca si aggiorna visualizzando la categoria selezionata.

Ticket correlati

Collegamenti a Richieste, Incidenti, Problemi e Issue e i documenti che sono stati aperti a causa del documento o che sono stati risolti tramite il documento.

Proprietà

Indicate le proprietà documento aggiuntive selezionate nel modello documento. Per impostazione predefinita, vengono sempre visualizzati la data di modifica e l'ID del documento.

Commenti

Elenca i commenti sul documento ricevuti dagli utenti. I commenti includono anche il nome del contatto, l'indirizzo di posta elettronica e la data.

Valuta e commenta

Fornisce commenti di completamento e feedback su quanto è stato utile il documento per risolvere il problema. È possibile valutare l'utilità del documento, in base alle domande seguenti:

- Questo documento risolve il problema?
- Quanto è stato utile questo forum?

Inoltre, è possibile aggiungere un commento e assegnarlo ad un altro analista per il completamento utilizzando uno dei seguenti tipi di commenti:

- Collegamento interrotto
- Destinato alla pubblicazione
- Destinato al ritiro
- Informazioni errate
- Informazioni mancanti
- Nuovo contenuto consigliato
- Revisione
- Soluzione non funzionante

Nella sezione Opzioni pagina è possibile effettuare le seguenti azioni:

- Modifica
- Aggiungi/Rimuovi segnalibro
- Sottoscrivi
- Valuta e commenta
- Posta elettronica
- Nuovo forum
- Nuovo Incidente
- Nuovo Incidente basato su questo documento
- Versione stampabile

Ulteriori informazioni:

Creazione di un tipo di commento (a pagina 996)
Configurazione di policy self-service (a pagina 1046)

Annunci

Gli annunci offrono un metodo veloce per fornire soluzioni per i problemi. Gli annunci forniscono una soluzione a problemi diffusi e per rispondere alle chiamate al Service Desk.

Gli annunci correnti vengono visualizzati nel riquadro destro della finestra principale di CA SDM quando ci si connette al sistema per la prima volta.

Ordinamento dei documenti

È possibile ordinare i documenti in base a vari criteri.

Per ordinare i documenti:

1. Nella scheda Conoscenza, selezionare un nodo della struttura dall'elenco delle categoria nel riquadro sinistro.
2. Espandere il nodo e fare clic su una categoria.

   Viene visualizzata la pagina Elenco documenti.
3. È possibile ordinare i documenti secondo i seguenti criteri utilizzando l'opzione Ordina per elenco:
   - Classificazione FAQ
   - N. di accessi
   - Documenti modificati di recente
   - Conteggio soluzioni

   I documenti vengono visualizzati nell'ordine selezionato.

Ricerca dei documenti

È possibile categorizzare i documenti della conoscenza per permettere ai clienti di ricercare informazioni basate sulle domande frequenti (FAQ). Se si seleziona una categoria conoscenza, vengono visualizzate anche le sottocategorie e i documenti della conoscenza correlati. È possibile selezionare il documenti che si desidera visualizzare oppure una sottocategoria per limitare ulteriormente la ricerca.

Viene visualizzato un elenco dinamico dei documenti maggiormente utilizzati che consente di migliorare le funzionalità self-service.

Nota: gli utenti possono specificare i criteri relativi ad un elemento di interesse e il motore di ricerca individuerà i documenti della conoscenza corrispondenti, visualizzandoli nella pagina dei risultati di ricerca sotto forma di set di collegamenti ai "documenti consigliati". La query di ricerca può essere definita anche come parola chiave o set di parole (o frase) che identificano il concetto desiderato che potrebbe essere contenuto in uno o più documenti. Per ulteriori informazioni, vedere Creazione di nuovi documenti consigliati (a pagina 1033).

Applicazione di segnalibri ai documenti

È possibile creare un segnalibro per i documenti a cui si accede più frequentemente. Dopo la creazione del segnalibro, il documento viene aggiunto all'elenco dei segnalibri. Questo elenco consente di trovare rapidamente i documenti che si visualizzano più frequentemente. Una volta aggiunto un documento all'elenco dei segnalibri, nel campo del segnalibro viene appare un pulsante Rimuovi. È possibile rimuovere i segnalibri dall'elenco quando non vi si accede più con la stessa frequenza.

Nella cartella Segnalibri personali sono memorizzati i collegamenti ai documenti di frequente consultazione. Quando si fa clic su Segnalibri personali nel riquadro Categoria della scheda Conoscenza, viene visualizzato un elenco dei documenti con segnalibri nel riquadro Elenco documenti di conoscenza.

Incidenti e problemi

I clienti hanno talvolta dei problemi che non possono essere risolti semplicemente ricercando la conoscenza. L'archivio della conoscenza non contiene soluzioni immediate a tutti i problemi. I clienti con problemi che non possono essere risolti possono creare un incidente che viene successivamente inviato all'analista per ulteriori analisi. L'incidente descrive il problema e può talvolta essere basata su un documento della conoscenza esistente. Più informazioni si aggiungono a un incidente e più semplice sarà per l'analista risolverlo.

Gestione della conoscenza supporta molte attività definite da ITIL, comprese le seguenti:

- Gestione degli incidenti
  - Le ricerche nell'archivio della conoscenza possono essere utilizzate come aiuto per ricercare errori conosciuti durante l'indagine e la diagnosi degli incidenti
  - Categorizzazione degli incidenti
- Gestione dei problemi
  - Accesso alle informazioni sugli errori conosciuti come aiuto nel processo di individuazione dei problemi per ottenere la risoluzione nel caso in cui il problema si sia già verificato
  - Gestione e fornitura dell'accesso alle informazioni sulle soluzioni e workaround
  - Registrazione delle informazioni relative a procedure, istruzioni di lavoro, script di diagnostica ed errori conosciuti, con il supporto di contenuto, strumenti di modifica, misurazione e un processo di approvazione definibile per lo sviluppo delle risoluzioni
  - Analisi dei problemi tramite il collegamento e l'analisi degli incidenti

Documenti e utenti

Nell'interfaccia documenti della conoscenza, a cui si accede dal nodo Documenti della conoscenza presente nel contatore CA SDM, tutti gli utenti del sistema possono visualizzare la cartella della posta in arrivo e i commenti di completamento. L'amministratore gestisce i propri documenti non assegnati/non indicizzati, le policy di durata del documento automatizzati e i forum degli utenti.

Posta in arrivo dei documenti

Knowledge Documents Inbox (e Posta in arrivo gruppo) presente nel contatore CA SDM contiene i documenti assegnati all'utente o al gruppo dell'utente. È il repository centrale per i documenti in tutti gli stati, compresi documenti bozza e bozze di rielaborazione salvati e assegnati.

Si tratta di un container per le attività giornaliere ed è molto utile per gestire il processo di approvazione. I documenti creati o aggiornati vengono spostati nella cartella Posta in arrivo del proprietario. Le voci visualizzate nella posta in arrivo richiedono l'attenzione dell'utente durante il processo di pubblicazione. Finché non vengono pubblicate, le voci della posta in arrivo potrebbero non apparire come soluzioni e non venire aggiunte all'archivio della conoscenza. Controllare regolarmente la posta in arrivo per verificare se ci sono nuovi documenti.

Visualizzazione di commenti di completamento

La cartella della posta in arrivo relativa ai commenti di completamento nel contatore dei documenti della conoscenza CA SDM contiene i commenti assegnati all'utente o al suo gruppo.

Nella pagina Elenco Commenti è possibile visualizzare le informazioni di riepilogo relative ai commenti di completamento dell'utente.

Per visualizzare i commenti di completamento, selezionare Documenti della conoscenza, Commenti di completamento.

Attributi documento

L'impostazione degli attributi documento consente di gestire i documenti nel pool della conoscenza. È possibile aggiornare gli attributi documento per assegnare un nuovo esperto argomento o proprietario al documento. È possibile specificare anche la data in cui il documento sarà disponibile nell'archivio della conoscenza e la sua data di scadenza. Se si selezionano più modelli documento, è possibile modificare l'aspetto di ciascun documento.

Autorizzazioni del documento

È possibile impostare, visualizzare e modificare le autorizzazioni di un documento. Queste autorizzazioni possono essere assegnate a gruppi di persone diverse. Quando si impostano le autorizzazioni, è possibile decidere di ereditare le autorizzazioni dalla categoria principale di documento oppure specificare nuove impostazioni. Per impostazione predefinita, i documenti ereditano le autorizzazioni dalla loro categoria principale. Questa impostazione predefinita gestisce le autorizzazioni di accesso a livello di categoria anziché di documento.

Importante. Quando si crea un documento della conoscenza, accertarsi che le autorizzazioni del documento contengano gli utenti che potrebbero essere assegnati successivamente al documento tramite il processo di approvazione. Quando un gruppo è assegnato a un documento, è possibile che gli utenti appartenenti a tale gruppo non abbiano l'autorizzazione a visualizzare il documento. Se il documento è assegnato a un utente specifico, i vincoli partizione dati predefiniti consentono all'utente di visualizzare il documento.

Categorie conoscenza

Assegnare ciascun documento a una categoria primaria. Ad esempio, qualsiasi conoscenza correlata a Microsoft Word deve essere aggiunta alla categoria di Microsoft Word. In aggiunta, Gestione della conoscenza consente di associare un documento a più categorie secondarie e ad altri documenti. In questo modo, un documento può essere classificato in diverse categorie applicabili e può fornire risultati di ricerca più corretti. Dopo la creazione di un collegamento documento, viene visualizzato anche un collegamento *Vedi anche* quando si visualizza uno dei documenti collegati. Il collegamento *Vedi anche* consente di passare direttamente da un documento collegato a un altro.

Autorizzazioni allegati

È possibile gestire le autorizzazioni degli allegati tramite la Libreria allegati, nodo Repository nella scheda Amministrazione. Le autorizzazioni per le cartelle repository possono essere impostate in base alle proprie esigenze aziendali.

Nota: un documento può disporre di diverse autorizzazioni rispetto agli allegati collegati al documento.

Aggiunta di un allegato di documento

Quando si lavora su un documento della conoscenza, è possibile allegare file o URL supplementari al documento. Questi file o URL supplementari consentono di accedere facilmente alle informazioni tradizionali correlate ai documenti della conoscenza. I file degli allegati vengono memorizzati in un repository.

Utilizzare la scheda Allegati per gestire file e URL allegati al documento corrente. Nei documenti creati utilizzando il modello predefinito Incorporato - Documento di conoscenza o Incorporato - Struttura conoscenza, i collegamenti agli allegati vengono visualizzati sotto all'intestazione "Allegati".

Nota: la scheda Allegati visualizza solo i documenti pubblicati. Per i documenti non pubblicati, la scheda Allegati visualizza i riquadri Repository, File e Allegati, e un elenco degli URL e file correntemente allegati al documento.

Per aggiungere un allegato file a un documento

1. Aprire il documento per apportare le modifiche.
2. Fare clic sulla scheda Allegati.
3. Immettere l'URL che si desidera allegare.
4. Eseguire una delle operazioni seguenti:
   - Fare clic su Allega file per aggiungere un file dal sistema.
   - Fare clic su Allega file da libreria per selezionare il nome del file che si desidera allegare dall'elenco Repository.

   Il nome viene visualizzato nella scheda Allegati.

Visualizzazione della cronologia di un documento

È possibile rivedere una registrazione di tutte le azioni effettuate su un documento.

Per visualizzare la cronologia di un documento, selezionare la scheda Cronologia nella pagina Aggiorna documento.

Viene visualizzato un elenco di eventi che mostra i dettagli di ciascun evento. Le informazioni visualizzate nella scheda Cronologia sono puramente di riferimento e non possono essere modificate.

Notifiche documento

In CA SDM, è possibile impostare un elenco di utenti, chiamati contatti, a cui inviare una notifica nel caso in cui si verifichino determinati eventi. Il processo di notifica segnala agli utenti lo stato di modifica di un documento e li tiene aggiornati sul suo avanzamento. È possibile inviare agli utenti solo le notifiche specificate per il documento.

Modifiche ai documenti

Quando un documenti arriva nella cartella Posta in arrivo nel contatore, gli utenti possono eseguire le loro attività assegnate modificando e salvando i documenti in base ai propri ruoli. Ad esempio, un analista può essere il responsabile del contenuto tecnico del documento, mentre un altro è il responsabile della sua formattazione.

Tutti gli utenti che dispongono delle autorizzazioni complete per il documento possono modificare il documento. Il proprietario corrente ha pieno controllo del documento, ma non dispone di autorizzazioni in scrittura esplicite. Solo il proprietario può cambiare la proprietà del documento, nella scheda Attributes.

Come gestire i privilegi dei ruoli e la visibilità dei documenti

È possibile impostare autorizzazioni di protezione Gestione della conoscenza gestendo i privilegi dei ruoli per gli utenti del proprio ambiente. Queste autorizzazioni permettono di specificare gli elementi a cui gli utenti possono accedere quando desiderano visualizzare o creare conoscenza e le modalità di autenticazione che devono seguire per accedere al sistema.

Per gestire i privilegi dei ruoli e la visibilità dei documenti per Gestione della conoscenza, effettuare le seguenti operazioni:

1. Dalla scheda Amministrazione, selezionare Gestione ruoli e protezione, Gestione ruoli, Elenco ruoli.

   Viene visualizzata la pagina Elenco ruoli.

2. Selezionare il ruolo desiderato; ad esempio Gestione della conoscenza.

   Le pagine Dettagli ruolo e Aggiorna ruolo contengono le seguenti schede:

   Gestione della conoscenza

   Specifica i privilegi Gestione della conoscenza assegnati al ruolo.

   Visibilità documento SC

   Specifica gli stati dei documenti che il ruolo è autorizzato a visualizzare; ad esempio Bozza, Ritirato e Pubblicato.

3. Completare le pagine delle schede e salvare le modifiche.

   Vengono impostati i privilegi di protezione e dei ruoli.

Nota: per ulteriori informazioni sull'impostazione della protezione e la definizione dei ruoli, vedere la *Guida in linea*.

Contenuto azione

È possibile creare un "contenuto azione" (un URL live) da inserire nel campo Risoluzione di un documento della conoscenza che, una volta selezionato dall'utente finale, crea un Incidente o esegue un'altra azione. Tramite il contenuto azione è possibile ottenere un considerevole livello di definizione e classificazione senza che l'utente se ne accorga.

La procedura per inserire un collegamento "contenuto azione" live in un documento è semplice e non richiede l'inserimento di codice. L'editor HTML di Gestione della conoscenza gestisce la creazione del codice HTML.

Nota: il contenuto azione è utilizzato principalmente per l'interazione con applicazioni esterne.

Ulteriori informazioni:

Visualizzazione dei contenuti azione (a pagina 977)
Creazione di contenuto azione (URL azione) (a pagina 978)
Creazione di contenuto azione (HTMPL interno) (a pagina 979)
Modifica del contenuto azione (a pagina 979)
Ricerca del contenuto azione (a pagina 980)

Visualizzazione dei contenuti azione

È possibile visualizzare i dettagli degli URL delle azioni in tempo reale che permettono di definire azioni per gli utenti finali. Gestione della conoscenza permette di collegare i documenti della conoscenza con attività automatiche, in modo da poter incorporare gli script self-service nei documenti della conoscenza.

Per visualizzare il contenuto azione:

1. Nella scheda Amministrazione accedere a Conoscenza, Contenuto azione.

   Viene visualizzata la pagina Elenco contenuto azione.

2. Questa pagina visualizza i dettagli dell'azione e le opzioni di esecuzione.

   Nome

   Visualizza il nome del contenuto azione.

   Codice

   Consente di specifica il codice HTML che collega il contenuto azione al documento.

   URL azione

   Consente di specificare il collegamento URL che esegue una determinata azione, come aprire un sito Web o un modulo.

   Cerca

   Effettua la ricerca di elementi per nome.

   Mostra filtro

   Consente di ricercare gli elementi nella pagina Elenco Commenti. È possibile compilare uno o più campi di ricerca e fare clic su Cerca. Nella pagina Elenco contenuto azione vengono visualizzati gli elementi che corrispondono alle norme selezionate.

   Crea nuovo

   Crea un collegamento al contenuto azione.

3. Ricerca o contenuto azione utilizzabili con Gestione della conoscenza e Support Automation.

   Vengono visualizzati i risultati della ricerca.

Creazione di contenuto azione (URL azione)

È possibile creare Contenuto azione per documenti della conoscenza. Questi URL di azioni possono avviare un sito Web live accessibile a tutti gli utenti del sistema. È inoltre possibile collegare URL di azioni ad attività automatiche sul server (qualsiasi server su cui è in esecuzione il daemon SC) ed è possibile incorporare questi script in documenti della conoscenza, documenti struttura, modelli di documento e forum della conoscenza.

Per creare contenuto azione (URL azione)

1. Nella scheda Amministrazione accedere a Conoscenza, Contenuto azione.

   Viene visualizzata la pagina di elenco Contenuto azione.

2. Fare clic su Crea nuovo.

   Viene visualizzata la pagina Crea nuovo contenuto azione.

3. Completare i campi. Di seguito si riporta una breve descrizione dei campi seguenti:

   Codice

   Specifica un identificatore unico per questo elemento di contenuto azione.

   Utilizza HTMPL interno

   Crea un collegamento interno (a pagina 979)nell'applicazione che passa dinamicamente informazioni, quali il nome utente e l'ID sessione, da documenti della conoscenza ad applicazioni di terze parti. Non selezionare questa opzione.

   URL azione

   Specifica un URL che collega a una pagina Web, modello Web o script automatico, ad esempio http://www.ca.com.

   Fare clic su Salva.

   Viene creato il contenuto azione.

Creazione di contenuto azione (HTMPL interno)

È possibile creare Contenuto azione per documenti della conoscenza. Questi URL di azioni possono avviare script self service e anche applicazioni di terze parti. Questo collegamento viene generato dinamicamente e trasferisce automaticamente attributi sull'utente, quale il nome utente, all'applicazione di destinazione (http://www.ca.com?USERNAME=BBB, ad esempio). Gli attributi dell'utente sono specificati in un file HTMPL.

Per creare contenuto azione con un file HTMPL interno

1. Creare un file HTMPL interno che passa dati all'applicazione di destinazione.

   Nota: il file act_content_sample.htmpl è disponibile nella seguente posizione: NX_ROOT\bopcfg\www\htmpl\default.

2. Salvare il file HTMPL nella seguente posizione: NX_ROOT\site\mods\www\htmpl\default directory.

3. Nella scheda Amministrazione, accedere a Conoscenza, Contenuto azione.

   Viene visualizzata la pagina di elenco Contenuto azione.

4. Fare clic su Crea nuovo.

   Viene visualizzata la pagina Crea nuovo contenuto azione.

5. Compilare il seguente campo:

   Codice

   Specifica un identificatore unico per questo elemento di contenuto azione.

6. Selezionare la casella di controllo Utilizza HTMPL interno.

7. Specificare il file HTMPL appropriato nel campo URL azione, ad esempio: act_content_sample.htmpl

   Nota: è possibile utilizzare script di Support Automation utilizzando il formato *SA_SCRIPT=[ID script self-service]* nell'URL.

8. Fare clic su Salva.

   Viene creato il contenuto azione. Quando l'utente fa clic sul collegamento Contenuto azione all'interno di un documento della conoscenza, gli attributi dell'utente, quali il nome utente, vengono passati dinamicamente all'applicazione di destinazione.

Modifica del contenuto azione

È possibile modificare contenuto azione già creato nella pagina Elenco Contenuto azione.

Per modificare il contenuto azione

1. Nella scheda Amministrazione, selezionare Conoscenza, Contenuto azione.

   Viene visualizzata la pagina Elenco contenuto azione.

2. Selezionare l'elemento da modificare.

   Viene visualizzata la pagina Dettagli contenuto azione.

3. Fare clic su Modifica.

   Viene visualizzata la pagina Aggiorna contenuto azione.

4. Modificare i campi in modo appropriato.
5. Fare clic su Salva.

   Il contenuto azione viene aggiornato.

Ricerca del contenuto azione

Per visualizzare solo gli elementi desiderati, è possibile immettere criteri di ricerca per filtrare l'Elenco contenuto azione. È anche possibile effettuare la ricerca di elementi individuali da visualizzare o modificare.

Per eseguire la ricerca di contenuto azione

1. Nella scheda Amministrazione, selezionare Conoscenza, Contenuto azione.

   Viene visualizzata la pagina Elenco contenuto azione.

2. Fare clic su Mostra filtro.

   Viene visualizzato il filtro di ricerca.

3. Compilare uno o più campi di ricerca.

   Nome

   Identifica il nome dell'elemento di contenuto azione.

   Stato

   Indica se l'elemento è attivo o non attivo.

   Codice

   Specifica un identificatore unico per questo elemento di contenuto azione.

   URL Gestione della conoscenza

   Specifica che l'URL azione collega a una pagina Web interna (.htmpl).

4. (Opzionale) Fare clic su Altro.

   Vengono visualizzati altri campi per restringere ulteriormente il numero di elementi visualizzati nell'Elenco contenuto azione

5. Fare clic su Cerca.

   Nella pagina Elenco contenuto azione vengono visualizzati gli elementi che corrispondono ai criteri selezionati. È possibile selezionare un elemento per visualizzarlo o modificarlo.

Nota: è possibile esportare i risultati sotto forma di elenco in Excel in modo che possano essere usati esternamente a CA SDM facendo clic sul pulsante Esporta nella pagina Elenco.

Processo di approvazione dei documenti

Per gli amministratori che desiderano controllare la gestione dell'archivio della conoscenza, è indispensabile poter personalizzare il processo di modifica e approvazione dei documenti. È possibile creare modelli di processo di approvazione che specificano come, quando e quale documento dipendente può essere modificato e pubblicato pubblicamente. I modelli del processo di approvazione possono specificare i vari processi di approvazione più idonei all'ambiente aziendale. In seguito, è possibile modificare il processo di approvazione implementato per renderlo più semplice o complesso.

Gestione processo di approvazione consente di definire i modelli del processo di approvazione. Per impostazione predefinita, viene usato il modello di processo di approvazione incorporato. Tuttavia, è possibile anche creare un nuovo modello o modificarne uno esistente. Quando si crea un modello di processo di approvazione, è necessario definire gli stati e aggiungere attività al modello. Il processo di approvazione include una serie di attività da eseguire sul documento della conoscenza. Il proprietario a cui viene assegnata un'attività nel modello del processo di approvazione ha il compito di eseguire ciascuna attività.

I seguenti stati sono i vari stati che possono essere associati al documento durante le fasi del processo di approvazione:

Bozza

Indica che si tratta di un nuovo documento.

Pubblicato

Indica che un documento che ha superato tutto il ciclo di approvazione ed è diventato parte dell'archivio della conoscenza visualizzabile.

Rework-Draft Version (Versione release/prodotto)

Indica che si tratta di una versione di rielaborazione di una copia di un documento che è stata sostituita nell'archivio della conoscenza dopo la verifica e ripubblicazione.

Ritirato

Indica che un documento ha raggiunto la data di scadenza. È possibile anche creare stati personalizzati e associarli successivamente alle attività.

Gestione processo di approvazione

Gli amministratori della conoscenza possono utilizzare Gestione processo di approvazione per eseguire le seguenti azioni:

- Stabilire quali gruppi possono leggere un documento della conoscenza e quali possono scrivere (o modificare) il documento della conoscenza.
- Identificare le attività in un modello di processo di approvazione che determinano il ciclo di vita di documenti creati con il modello.
- Definire i vari stati ai quali può essere associato il documento durante il processo di approvazione.

Importante. Quando si crea un documento della conoscenza, accertarsi che le autorizzazioni del documento contengano gli utenti che potrebbero essere assegnati successivamente al documento attraverso il processo di approvazione. Gli utenti di tale gruppo non dispongono necessariamente delle autorizzazioni per visualizzare il documento. Se il documento è assegnato a un utente specifico, i vincoli di partizione dati predefiniti consentono all'utente di visualizzare il documento.

Definizione di un processo di approvazione per la modifica del documento

Gli amministratori della conoscenza possono specificare quali utenti possono modificare i documenti prima del processo di approvazione e dopo la pubblicazione.

Nota: gli utenti con autorizzazioni di lettura/scrittura complete possono modificare i documenti pubblicati.

Per definire un processo di approvazione per la modifica di un documento:

1. Nella scheda Amministrazione, accedere a Conoscenza, Gestione processo di approvazione, Impostazioni processo di approvazione.

   Viene visualizzata la pagina Impostazioni processo di approvazione.

2. Specificare quali utenti possono modificare i documenti *prima* della loro pubblicazione. Selezionare una delle opzioni riportate di seguito:

   I documenti possono essere modificati da un assegnatario di attività, da un proprietario oppure dagli utenti che dispongono delle viste del tipo di accesso appropriate

   Indica che i seguenti contatti possono modificare i documenti:

   - Un contatto assegnato all'attività corrente
   - Un contatto specificato come proprietario del documento per l'attività corrente
   - Un manager della conoscenza
   - Un amministratore di sistema

   I documenti possono essere modificati dagli utenti con autorizzazioni complete

   Indica che qualsiasi utente con autorizzazioni di scrittura per il documento può modificarlo.

3. Specificare quali utenti possono modificare i documenti *dopo* la loro pubblicazione. Selezionare una delle opzioni riportate di seguito:

   Gli utenti con autorizzazioni complete possono modificare i documenti dopo la loro pubblicazione

   Indica che un utente con autorizzazioni complete può modificare i documenti pubblicati.

   Gli utenti con autorizzazioni complete possono modificare gli attributi di un documento pubblicato

   Indica che qualsiasi utente con autorizzazioni di scrittura per il documento può modificare solo gli attributi di documenti pubblicati, come gli elementi della configurazione o i prodotti.

   Per consentire la modifica, è necessario prima annullare la pubblicazione del documento

   Indica che l'utente deve annullare la pubblicazione di un documento prima di modificarlo.

   Fare clic su Salva.

   Viene definito il processo di approvazione.

Creazione di un modello di processo di approvazione

Le attività nel modello di processo di approvazione definiscono il ciclo di vita dei documenti creati tramite il modello.

Nota: in caso di installazione dell'opzione multi-tenancy, selezionare il titolare appropriato dall'elenco a discesa. L'opzione pubblica (condivisa) consente di creare l'oggetto per tutti i titolari.

Per creare un modello processo di approvazione

1. Nella scheda Amministrazione selezionare Conoscenza, Gestione processo di approvazione, Modelli processo di approvazione.

   Viene visualizzata la pagina Elenco Modelli di processo approvazione.

2. Fare clic su Crea nuovo.

   Viene visualizzata la pagina dei dettagli del modello processo di approvazione.

3. Immettere un nome e una descrizione per il modello.

4. Fare clic su Salva.

   La pagina Dettagli modello del processo di approvazione visualizza alcuni campi aggiuntivi.

5. Selezionare l'attività che si desidera eseguire quando si crea una nuova versione di rielaborazione del documento utilizzando il modello.

6. Selezionare l'attività che si desidera eseguire quando si annulla il ritiro di un documento creato utilizzando il modello.

7. Fare clic su Inserisci attività per creare un'attività da aggiungere al modello.

   Viene visualizzata la pagina Crea nuova attività.

8. Completare i campi. Di seguito si riporta una breve descrizione dei campi seguenti:

   Attività

   Assegna un nome all'attività.

   Assegnatario

   Assegna una persona all'attività. È possibile anche fare clic sull'icona Cerca per selezionare un nome.

   Nota: al termine della creazione dell'attività, è possibile aggiungere un elenco alternativo di assegnatari (a pagina 985).

   Fare clic su Salva.

   Viene creato il modello del processo di approvazione.

Ulteriori informazioni:

Aggiunta di assegnatari alternativi a un'attività (a pagina 985)
Modifica di un modello processo di approvazione (a pagina 985)
Ricerca di un modello processo di approvazione (a pagina 986)

Aggiunta di assegnatari alternativi a un'attività

È possibile aggiungere assegnatari alternativi quando si modifica un'attività.

Per aggiungere assegnatari alternativi a un'attività:

1. Selezionare l'attività da modificare nella pagina Elenco Modelli di processo approvazione.

   Viene visualizzata la pagina Dettagli attività.

2. Modificare i campi in modo appropriato.
3. Fare clic sul pulsante Aggiungi nella pagina Elenco Assegnatari.

   Viene visualizzata la pagina Crea nuovo assegnatario.

4. Nel campo Assegnatario, immettere il nome della persona a cui si desidera assegnare l'attività oppure fare clic sull'icona Cerca per selezionare il nome.
5. Ripetere le operazioni della fase 4 più volte per creare un elenco di assegnatari alternativi.
6. Fare clic su Salva.

   L'assegnatario alternativo viene aggiunto all'attività.

Modifica di un modello processo di approvazione

È possibile modificare un modello processo di approvazione.

Per modificare un modello processo di approvazione

1. Nella scheda Amministrazione selezionare Conoscenza, Gestione processo di approvazione, Modelli processo di approvazione.

   Viene visualizzata la pagina Elenco Modelli di processo approvazione.

2. Selezionare il modello da modificare e fare clic sul nome corrispondente.

   Viene visualizzata la pagina dei dettagli del modello processo di approvazione.

3. Fare clic su Modifica.

   Viene visualizzata la pagina Aggiorna modello del processo di approvazione.

4. Modificare i campi in modo appropriato.
5. Fare clic su Salva.

   Il modello del processo di approvazione viene aggiornato.

Ricerca di un modello processo di approvazione

Per visualizzare solo gli elementi desiderati, è possibile immettere criteri di ricerca per filtrare la pagina Elenco Modelli di processo approvazione. È anche possibile effettuare la ricerca di elementi individuali da visualizzare o modificare.

Nota: in caso di installazione dell'opzione multi-tenancy, la pagina di elenco visualizzerà le impostazioni Titolare e Dati pubblici nel filtro di ricerca. L'opzione Dati pubblici può essere inclusa o esclusa per i dati del titolare: la ricerca viene eseguita unicamente per gli oggetti pubblici. Nelle pagine dei dettagli, selezionare il titolare appropriato dall'elenco. Se si seleziona <vuoto>, l'oggetto è pubblico.

Per eseguire la ricerca di un modello processo di approvazione

1. Nella scheda Amministrazione selezionare Conoscenza, Processo di approvazione, Modelli di processo approvazione.

   Viene visualizzata la pagina Elenco modelli di processo approvazione.
2. Fare clic su Mostra filtro.
3. Immettere i primi caratteri del nome del modello da ricercare.
4. (Opzionale) Fare clic su Altro.

   Vengono visualizzati ulteriori campi che consentono di limitare gli elementi che vengono visualizzati nella pagina Elenco Modelli di processo approvazione.
5. Fare clic su Cerca.

   Nella pagina Elenco Modelli di processo approvazione vengono visualizzati gli elementi che corrispondono ai criteri di ricerca selezionati. È possibile selezionare un elemento per visualizzarlo o modificarlo.

Nota: è possibile esportare i risultati sotto forma di elenco in Excel in modo che possano essere usati esternamente a CA SDM facendo clic sul pulsante Esporta nella pagina Elenco.

Definizioni di stato del documento

È possibile aggiungere ed eliminare stati di un documento definiti dall'utente nonché modificare nomi e descrizioni degli stati predefiniti di un documento.

Ulteriori informazioni:

Creazione dello stato di un documento (a pagina 987)
Ricerca degli stati di documento (a pagina 987)
Modifica dello stato di un documento (a pagina 988)

Creazione dello stato di un documento

È possibile creare uno stato per i documenti della conoscenza nel sistema CA SDM.

Per creare un nuovo stato documento

1. Nella scheda Amministrazione selezionare Conoscenza, Gestione processo di approvazione, Stati documento.

   Viene visualizzata la pagina Elenco di stato documento.

2. Fare clic su Crea nuovo.

   Viene visualizzata la pagina dei dettagli di stato documento.

3. Immettere un nome e una descrizione per lo stato.

4. Fare clic su Salva.

   Viene creato lo stato del documento.

Ricerca degli stati di documento

Per visualizzare solo gli elementi desiderati, è possibile immettere criteri di ricerca per filtrare l'Elenco stati documento. È anche possibile effettuare la ricerca di elementi individuali da visualizzare o modificare.

Per eseguire la ricerca dello stato di un documento

1. Nella scheda Amministrazione selezionare Conoscenza, Gestione processo di approvazione, Stati documento.

   Viene visualizzata la pagina Elenco di stato documento.

2. Fare clic su Mostra filtro.

3. Immettere i primi caratteri del nome dello stato da ricercare.

4. (Opzionale) Fare clic su Altro.

   Vengono visualizzati ulteriori campi in cui è possibile limitare il numero di elementi visualizzati nella pagina Elenco di stato documento.

5. Fare clic su Cerca.

   La pagina Elenco di stato documento mostra gli elementi che corrispondono ai criteri di ricerca specificati. È possibile selezionare un elemento per visualizzarlo o modificarlo.

Nota: è possibile esportare i risultati sotto forma di elenco in Excel in modo che possano essere usati esternamente a CA SDM facendo clic sul pulsante Esporta nella pagina Elenco.

Modifica dello stato di un documento

È possibile modificare lo stato di un documento.

Per modificare lo stato di un documento:

1. Nella scheda Amministrazione selezionare Conoscenza, Gestione processo di approvazione, Stati documento.

   Viene visualizzata la pagina Elenco di stato documento.

2. Selezionare lo stato da modificare e fare clic sul nome corrispondente.

   Viene visualizzata la pagina dei dettagli di stato documento.

3. Fare clic su Modifica.

   Viene visualizzata la pagina di aggiornamento dello stato documento.

4. Modificare i campi Stato e Descrizione se richiesto.
5. Fare clic su Salva.

   Lo stato del documento viene aggiornato.

Policy automatiche

Nel processo di approvazione del documento della conoscenza gli amministratori hanno la facoltà di automatizzare determinate attività sulla base delle policy del ciclo di vita del documento e delle azioni definite. L'automazione delle attività consente agli utenti finali di risolvere più rapidamente i problemi senza la necessità di contattare altre persone e con conseguenti vantaggi per le aziende.

Le policy automatizzate funzionano con eventi e macro.

Ulteriori informazioni:

Visualizzazione di policy automatiche (a pagina 989)
Modalità di impostazione delle policy automatiche (a pagina 990)
Creazione di una policy automatica (a pagina 991)
Modifica di una policy automatica (a pagina 992)
Pianificazione di policy automatiche (a pagina 992)
Visualizzazione di report relativi alle policy del ciclo di vita di un documento (a pagina 993)

Visualizzazione di policy automatiche

Una policy automatica descrive la condizione per cui i documenti vengono contrassegnati per la correzione e promossi per la pubblicazione o il ritiro attraverso le varie fasi del processo del ciclo di vita del documento. Ad esempio, è possibile specificare la policy predefinita "correzione collegamenti interrotti" che corrisponde ai documenti trovati nell'archivio della conoscenza con collegamenti interrotti. Il compito di correzione di un problema può essere assegnato ad un analista.

Nota: in caso di installazione dell'opzione multi-tenancy, la pagina di elenco visualizzerà le impostazioni Titolare e Dati pubblici nel filtro di ricerca. L'opzione Dati pubblici può essere inclusa o esclusa per i dati del titolare: la ricerca viene eseguita unicamente per gli oggetti pubblici. Nelle pagine dei dettagli, selezionare il titolare appropriato dall'elenco. Se si seleziona <vuoto>, l'oggetto è pubblico.

Per visualizzare policy automatiche, selezionare la scheda Amministrazione, Conoscenza, Policy automatiche, Policy.

Nella pagina Elenco policy automatiche vengono visualizzati i dettagli delle policy automatiche. È possibile modificare le policy predefinite oppure definire policy personalizzate. Ogni policy è associata ai seguenti componenti:

Query memorizzata

Contiene un insieme di macro Azione che vengono eseguite quando le policy identificano un documento corrispondente durante l'elaborazione. Dopo l'elaborazione, l'evento condizione della query memorizzata visualizza un report relativo alle policy del ciclo di vita di Gestione della conoscenza basato su ruoli nel contatore CA SDM.

L'amministratore è responsabile di monitorare i report per fornire feedback e raccomandazioni agli editor dei documenti appropriati.

Macro azione

Contiene codice che consente agli utenti di impostare la priorità o eseguire altre azioni. È possibile modificare le macro visualizzate in questo elenco oppure definirne di proprie.

Nota: è possibile esportare i risultati sotto forma di elenco in Excel in modo che possano essere usati esternamente a CA SDM facendo clic sul pulsante Esporta nella pagina Elenco.

Ulteriori informazioni:

Visualizzazione di report relativi alle policy del ciclo di vita di un documento (a pagina 993)
Pianificazione di policy automatiche (a pagina 992)

Modalità di impostazione delle policy automatiche

Gli amministratori possono impostare la funzionalità Policy automatiche attenendosi alla seguente procedura:

1. (Obbligatorio) In Pianificazione policy automatiche è necessario definire un'elaborazione batch che verrà eseguita sul server in background allo scopo di presentare i dati necessari per visualizzare i report relativi alle policy del ciclo di vita di Gestione della conoscenza. Questa procedura riguarda anche la scheda Report della conoscenza.

   Nota: per maggiori informazioni sulle policy automatiche, consultare la *Guida all'implementazione*.

2. (Obbligatorio) Per la gestione di ruoli e protezione, definire la fase in corrispondenza della quale gli utenti possono visualizzare e ricercare documenti durante il ciclo di vita nella scheda Visibilità documento della conoscenza di Gestione ruoli.

3. Nella pagina Elenco policy automatiche, è possibile modificare le policy predefinite o definirne di proprie.

   Nota:per le nuove policy, l'amministratore deve includere il campo Ignora policy del ciclo di vita nella query memorizzata. In caso contrario non verrà visualizzato nella scheda Attributi.

Creazione di una policy automatica

È possibile creare una policy automatica che viene attivata quando viene effettuata un'azione, ad esempio viene pubblicato o ritirato un documento dall'archivio della conoscenza.

Nota: in caso di installazione dell'opzione multi-tenancy, selezionare il titolare appropriato dall'elenco a discesa. L'opzione pubblica (condivisa) consente di creare l'oggetto per tutti i titolari.

Per creare una policy automatica

1. Nella scheda Amministrazione, accedere a Conoscenza, Policy automatiche, Policy.

   Viene visualizzata la pagina Crea Nuova policy automatica.

2. Immettere un nome e la descrizione della policy nei campi appropriati.
3. Immettere un nome di query memorizzata oppure selezionarne uno con l'icona di ricerca.
4. Fare clic su Aggiungi azione.

   Viene visualizzata la pagina Elenco macro.

5. Nella pagina Elenco macro, selezionare una delle macro azione predefinite oppure definirne di proprie (facendo clic su Crea nuovo).

   La macro azione viene visualizzata nell'elenco Informazioni azione della pagina Crea nuova policy automatica.

   Nota: è possibile eliminare una macro azione; fare clic con il pulsante destro del mouse sul nome e selezionare Elimina dal menu di scelta rapida.

6. Fare clic su Salva.

   La nuova policy viene visualizzata nell'elenco delle policy automatiche.

7. (Facoltativo) Fare clic con il pulsante destro del mouse sul titolo per modificare una policy.

   La policy selezionata viene visualizzata nella pagina di aggiornamento della policy, dove è possibile modificarla.

Modifica di una policy automatica

È possibile aggiornare una policy automatica.

Per modificare una policy automatica

1. Nella scheda Amministrazione, accedere a Conoscenza, Policy automatiche, Policy.

   Viene visualizzato l'Elenco policy automatiche.

2. Fare clic con il pulsante destro del mouse sulla policy da modificare, quindi selezionare Modifica dal menu di scelta rapida.

   Viene visualizzata la pagina Aggiorna policy automatica.

3. Modificare i campi di immissione in modo appropriato.
4. Fare clic su Salva.

   La policy viene aggiornata.

Pianificazione di policy automatiche

È possibile specificare la data e l'ora in cui viene eseguito il calcolo e l'esecuzione dell'elaborazione batch delle policy.

Per pianificare policy automatiche

1. Fare clic sulla scheda Amministrazione, quindi accedere a Conoscenza, Policy automatiche, Pianificazione.

   Viene visualizzata la pagina Policy automatiche.

2. Inserire i dati nei seguenti campi:

   Ultimo aggiornamento

   Selezionare la casella di controllo Esegui calcolo.

   Pianifica

   Specificare una data nella casella di testo o selezionarla nel calendario. È possibile selezionare l'intervallo di tempo in base al quale viene effettuato il calcolo e vengono eseguite le policy.

   Fare clic su Salva.

   Le policy vengono elaborate alla data e ora specificate.

Visualizzazione di report relativi alle policy del ciclo di vita di un documento

È possibile visualizzare i report relativi alle policy del ciclo di vita di un documento generati dalle policy automatiche.

Per visualizzare i report, selezionare la scheda Service Desk, Documenti della conoscenza, Policy automatiche, Policy.

Quando si seleziona una policy, nella pagina Elenco documenti vengono visualizzate le seguenti informazioni di riepilogo:

Nota: in caso di installazione dell'opzione multi-tenancy, la pagina di elenco visualizzerà le impostazioni Titolare e Dati pubblici nel filtro di ricerca. L'opzione Dati pubblici può essere inclusa o esclusa per i dati del titolare: la ricerca viene eseguita unicamente per gli oggetti pubblici. Nelle pagine dei dettagli, selezionare il titolare appropriato dall'elenco. Se si seleziona <vuoto>, l'oggetto è pubblico.

Titolo

Visualizza il titolo del documento che è contrassegnato per la correzione o promosso alla pubblicazione o al ritiro.

Policy/azioni

Visualizza il nome della policy e il contenuto azione definito per la policy.

Attributi

Visualizza le proprietà del documento su cui influisce la policy.

Controllo del documento della conoscenza

Aprire i documenti della conoscenza e aggiungere commenti, inviare la conoscenza e visualizzare i documenti struttura della conoscenza. Inoltre, è possibile specificare il contenuto e l'aspetto dei documenti selezionando un modello.

Gli amministratori possono effettuare le seguenti attività per controllare le interazioni degli utenti con i documenti:

- Definire i tipi di commenti (a pagina 994) che compaiono nei documenti della conoscenza e negli elenchi a discesa nell'interfaccia dell'utente finale
- Specificare le impostazioni (a pagina 1050) dei documenti relativamente ai commenti, all'invio della conoscenza e alla visualizzazione dei documenti

- Creare modelli di documenti (a pagina 1000) che specifichino il contenuto e l'aspetto dei documenti
- Esportare (o importare) il contenuto della conoscenza da un'altra risorsa o un altro sistema Per la configurazione con disponibilità avanzata, non è possibile eseguire l'esportazione o l'importazione dal server applicazioni mediante l'interfaccia utente Web di CA SDM. Per eseguire l'esportazione o l'importazione mediante un server applicazioni, eseguire l'utilità pdm_kit o pdm_ket, se il pacchetto è contenuto in un'unità condivisa UNC.
- Gestire le funzionalità delle versioni (a pagina 933) dei documenti
- Gestire la pianificazione dei documenti della conoscenza (a pagina 936)

Ulteriori informazioni:

Tipi commento (a pagina 994)
Modelli documento (a pagina 1000)
Come creare collegamenti documento della conoscenza (a pagina 1007)
Categorie conoscenza (a pagina 1009)
Report e metriche (a pagina 1019)
Cerca (a pagina 1021)
Indagine soluzione (a pagina 1047)

Tipi commento

Se l'analista nota un refuso o un problema relativo al contenuto in un documento, può aggiungere un commento per contrassegnare il documento per la correzione, quindi assegnare il problema a un altro analista per il completamento.

Gli amministratori hanno la facoltà di definire i tipi di commento visualizzati nelle varie visualizzazioni elenco nell'interfaccia dell'utente finale.

Visualizzazione dei tipi di commento

Al momento dell'apertura di un documento della conoscenza, l'utente può aggiungere un commento per contrassegnare il documento per la correzione, la promozione o il ritiro e molto altro ancora. Nella pagina Elenco Tipi di commento è possibile gestire i dettagli dei tipi di commento.

Per visualizzare questa pagina, selezionare la scheda Amministrazione, quindi Conoscenza, Documenti, Tipi di commento.

Nota: in caso di installazione dell'opzione multi-tenancy, la pagina di elenco visualizzerà le impostazioni Titolare e Dati pubblici nel filtro di ricerca. L'opzione Dati pubblici può essere inclusa o esclusa per i dati del titolare: la ricerca viene eseguita unicamente per gli oggetti pubblici. Nelle pagine dei dettagli, selezionare il titolare appropriato dall'elenco. Se si seleziona <vuoto>, l'oggetto è pubblico.

Viene visualizzata la pagina Elenco Tipi di commento che include le seguenti colonne:

Nome

Visualizza l'elenco di tipi di commento mostrato nei documenti e negli elenchi a discesa all'interno dell'interfaccia utente. È possibile modificare i seguenti tipi di commento predefiniti oppure definire tipi di commento personalizzati:

- Collegamento interrotto
- Destinato alla pubblicazione
- Contenuto non chiaro
- Difficile da trovare
- Commento generale
- Informazioni errate
- Informazioni mancanti
- Nuovo contenuto consigliato
- Revisione
- Soluzione non funzionante

Visualizza in Visualizzazione utente

Visualizza il commento in diverse visualizzazioni di elenco all'interno dell'interfaccia utente.

Completamento necessario

Specifica se all'utente è richiesto di rispondere a questo tipo di commento.

Tempo di completamento (giorni)

Definisce il numero di giorni entro il quale l'utente deve far seguito a questo tipo di commento.

Stato

Indica se il tipo di commento è attivo o inattivo.

In questa pagina sono disponibili i seguenti pulsanti:

Cerca

Effettua la ricerca di elementi per nome.

Mostra filtro

Consente di ricercare un commento nella pagina Elenco Commenti. Compilare uno o più campi di ricerca e fare clic su Cerca. La pagina Elenco Tipi di commento mostra i commenti che soddisfano i criteri di ricerca.

Cancella filtro

Cancella il filtro.

Crea nuovo

Crea un tipo di commento.

Nota: è possibile esportare i risultati sotto forma di elenco in Excel in modo che possano essere usati esternamente a CA SDM facendo clic sul pulsante Esporta nella pagina Elenco.

Creazione di un tipo di commento

È possibile specificare i tipi di commento mostrati nelle varie visualizzazioni elenco nell'interfaccia dell'utente finale.

Nota: in caso di installazione dell'opzione multi-tenancy, selezionare il titolare appropriato dall'elenco a discesa. L'opzione pubblica (condivisa) consente di creare l'oggetto per tutti i titolari.

Per creare un tipo di commento:

1. Nella scheda Amministrazione, selezionare Conoscenza, Documenti e Tipi commento.

   Viene visualizzata la pagina Elenco Tipi di commento.

2. Fare clic su Crea nuovo.

   Viene visualizzata la pagina Crea Nuovo tipo commento.

3. Compilare i campi in modo appropriato. Di seguito si riporta una breve descrizione dei campi seguenti:

   Tempo di completamento (giorni)

   Definisce il numero di giorni entro il quale l'utente deve far seguito a questo tipo di commento.

   Visualizza in Visualizzazione utente

   Visualizza il commento in diverse visualizzazioni di elenco all'interno dell'interfaccia utente.

   Completamento necessario

   Specifica se all'utente è richiesto di rispondere a questo tipo di commento.

   Fare clic su Salva.

   Il nuovo tipo di commento viene visualizzato nella pagina Elenco Tipi commento.

Modifica di un tipo di commento

È possibile aggiornare un tipo di commento già creato nella pagina Elenco Tipi commento.

Per modificare un tipo di commento:

1. Nell'elenco Tipo commento, effettuare una delle seguenti operazioni:
   - Selezionare un commento, quindi scegliere Modifica nella pagina Dettagli tipo commento.
   - Fare clic con il pulsante destro del mouse su un commento e selezionare Modifica dal menu di scelta rapida

   Viene visualizzata la pagina Dettagli tipo commento.
2. Compilare i campi in modo appropriato.
3. Fare clic su Salva.

   Il nuovo tipo di commento viene visualizzato nella pagina Elenco Tipi commento.

Notifiche documento

In CA SDM, è possibile impostare un elenco di utenti, chiamati contatti, a cui inviare una notifica nel caso in cui si verifichino determinati eventi. Il processo di notifica segnala agli utenti lo stato di modifica di un documento e li tiene aggiornati sul suo avanzamento. È possibile inviare agli utenti solo le notifiche specificate per il documento.

Impostazione di una notifica di commento di completamento

Nella pagina Elenco notifiche attività sono disponibili numerose notifiche attività predefinite che consentono di inviare automaticamente una notifica agli utenti quando viene loro assegnato un commento di completamento.

La coda Commenti di completamento presente nel contatore è il repository per i commenti di completamento assegnati e non assegnati.

Per impostare una notifica commento di completamento

1. Nella scheda Amministrazione, accedere a Notifiche, Notifiche attività.

   Viene visualizzata la pagina Elenco notifiche attività.
2. Selezionare *una* delle seguenti notifiche di attività:
   - Commento di completamento assegnato
   - Commento di completamento chiuso

   Viene visualizzata la pagina Dettagli notifica attività.

3. Fare clic su Modifica.

   Viene visualizzata la pagina Aggiorna notifica attività.

4. Modificare i campi in modo appropriato.
5. Fare clic su Salva.

   Viene visualizzata la pagina Dettagli notifica attività.

6. Fare clic su Chiudi finestra.

   La notifica attività modificata viene visualizzata nell'Elenco notifiche attività quando si visualizza nuovamente l'elenco.

Specificazione di impostazioni di documento

In qualità di amministratore di sistema, è possibile specificare impostazioni relative ai commenti, all'invio di documenti della conoscenza e alla visualizzazione di documenti della struttura della conoscenza.

Per specificare le impostazioni del documento

1. Dalla scheda Amministrazione fare clic su Conoscenza, Documenti, Impostazioni documento.

   Viene visualizzata la pagina Impostazioni documento.

2. Inserire i dati nei seguenti campi:

   Visualizzazione documento struttura conoscenza

   Consente di specificare la modalità di visualizzazione dei documenti della struttura conoscenza. Selezionare Apri in modalità Struttura (impostazione predefinita) per aprire la struttura della conoscenza direttamente o selezionare Apri in modalità Documento per aprire il documento nella visualizzazione documento. Se si apre in modalità Documento, fare clic su Visualizza per visualizzare la struttura della conoscenza.

   Commenti

   Specifica se è possibile inviare commenti per i documenti e visualizzare i commenti dei documenti. Selezionare una delle opzioni riportate di seguito:

   - **Consenti l'invio e la visualizzazione dei commenti (predefinito)**—Visualizza un campo Commento nella parte inferiore di un documento aperto in modo che gli utenti possano inviare commenti per il documento. È possibile visualizzare i commenti già associati al documento aperto.
   - **Consenti l'invio ma non la visualizzazione dei commenti**—Visualizza un campo Commento sulla destra di un documento aperto in modo che gli utenti possano inviare commenti per il documento. Non è possibile visualizzare i commenti già associati al documento aperto.

- **Non consentire né l'invio né la visualizzazione dei commenti**—Nega agli utenti la capacità di inviare o visualizzare commenti. Il campo Commento non viene visualizzato in un documento aperto.

Invia conoscenza

Definisce il repository per documenti inviati dagli utenti. L'elenco viene compilato con i nomi dei repository definiti nel riquadro Libreria allegati.

Prendere in considerazione le informazioni seguenti:

- Quando un analista crea un documento in una categoria con un proprietario ed assegna il documento al proprietario della categoria:

  Il proprietario della categoria diviene l'assegnatario e il proprietario del documento.

  Il proprietario della categoria riceverà una notifica di assegnazione del documento.

- Quando un analista crea un documento in una categoria senza proprietario ed assegna il documento al proprietario della categoria:

  Nessun assegnatario o proprietario viene associato al documento.

  La notifica di invio del documento della conoscenza verrà inviato in base alle impostazioni dell'amministratore.

- Quando un analista crea un documento e assegna il documento al proprietario della categoria:

  Tale utente diviene l'assegnatario e il proprietario.

  Non viene inviata alcuna notifica.

- Quando un dipendente o un cliente creano nuovi documenti, CA SDM esegue l'azione in base a quanto indicato nei primi due punti.

Dimensioni massime risoluzione

Definisce il limite massimo di caratteri ammessi nel campo Risoluzione per un documento.

Limiti: il numero massimo di caratteri consentito è 256.000.

Impostazione predefinita: 32.768.

Evita duplicazione documenti

Impone una ricerca di documenti simili quando l'utente crea un documento della conoscenza.

Notifica prima della scadenza

Definisce dopo quanti giorni il documento scade e viene inviata una notifica.

Impostazione predefinita: 7

Nota: questo valore si applica solo ai documenti aggiornati o creati in CA SDM. Se si effettua la migrazione di documenti da CA SDM r11,2 e le date di scadenza vengono impostate prima della migrazione, questa opzione non si applica, a condizione o fintanto che non si aggiorna il documento dopo la migrazione.

Fare clic su Salva.

È possibile applicare dei cambiamenti aprendo un documento della conoscenza oppure un documento della struttura della conoscenza.

Modelli documento

È possibile usare i modelli documento per controllare il formato e il contenuto predefinito dei documenti della conoscenza. Il modello documento di ciascun documento della conoscenza specifica le proprietà e l'aspetto del documento al momento della sua apertura. Per impostazione predefinita, ai nuovi documenti della conoscenza viene sempre associato un modello incorporato.

L'editor dei documenti consente di effettuare le operazioni seguenti:

- Creare un modello documento per poterlo successivamente associare a un documento nella scheda Contenuto della pagina Editor dei documenti
- Modificare il modello incorporato e altri modelli

  La modifica dei modelli consente di creare modelli da associare ai documenti. È possibile selezionare le opzioni Proprietà e modificare le sezioni dell'intestazione e del piè di pagina tramite l'editor HTML.
- Aggiornare i modelli documento di una versione precedente in modo che supportino le relazioni della conoscenza (a pagina 1006), come i collegamenti padre-figlio

Creazione di un modello di documento

Un modello di documento specifica il contenuto e l'aspetto dei documenti nell'archivio della conoscenza. È possibile applicare i parametri predefiniti:

- Incorporato—Documento della conoscenza
- Incorporato—Struttura della conoscenza
- Incorporato—Modifica rapida

Il prodotto utilizza modelli predefiniti quando si creano documenti della conoscenza e documenti della struttura della conoscenza a meno che non si creino modelli di documento e si associno ai propri documenti.

Nota: durante la creazione di un documento della conoscenza, selezionare il titolare appropriato dall'elenco a discesa. L'opzione pubblica (condivisa) consente di creare l'oggetto per tutti i titolari.

Per creare un modello di documento

1. Dalla scheda Amministrazione accedere a Conoscenza, Documenti, Modelli documento.

   Viene visualizzata la pagina Elenco modelli documento.

2. Fare clic su Crea nuovo.

   Viene visualizzata la pagina Crea Nuovo modello documento.

3. Inserire i dati nei seguenti campi:

   Modello

   (Richiesto) Definisce un nome univoco per il modello.

   Dettagli

   Consente di visualizzare il contenuto statico dei documenti creati tramite il modello corrente. Se si seleziona l'opzione Origine HTML, è possibile modificare il codice HTML del corpo direttamente in Corpo. Se si seleziona l'opzione Visualizzazione rapida, il campo Corpo risulta di sola lettura e visualizza il contenuto del corpo statico come compare al momento dell'esecuzione.

4. (Facoltativo) Fare clic su Imposta valori predefiniti.

   Viene visualizzata la pagina Modello valori predefiniti.

   È possibile definire valori predefiniti durante la creazione di un documento. Se si modifica il modello di un documento esistente, non ci sarà alcun impatto.

5. (Facoltativo) Nascondere Titolo, Riepilogo, Problema o Risoluzione nel modello.

   È possibile nascondere questi campi quando si desidera un documento semplice, come nel caso di un modello di domanda e risposta.

6. Fare clic su Modifica dettagli.

   Viene visualizzata la pagina Editor HTML e sarà possibile specificare il contenuto statico e il layout di documenti che usano il modello. È possibile modificare il codice utilizzando la barra degli strumenti per inserire tag segnaposto.

   Importante È possibile rimuovere relazioni della conoscenza, ad esempio padre, figlio e collegamenti relativi, eliminando i tag {TAG_PARENT} e {TAG_RELATED} dal modello.

7. Fare clic su OK.

   Il campo Dettagli mostra il contenuto aggiornato.

8. (Opzionale) Fare clic su Visualizzazione rapida.

   Mostra il contenuto come compare in documenti basati sul modello.

9. (Opzionale) Fare clic su Visualizzazione HTML.

   Mostra il contenuto come codice HTML.

10. Fare clic su Salva.

    Viene visualizzata la pagina Dettagli modello documento.

11. Fare clic su Chiudi finestra.

    Nuovi documenti che usano il modello mostrano il nuovo contenuto e layout.

    Visualizzando di nuovo l'elenco, viene visualizzato il nome del modello nell'elenco modelli.

Nota: modifiche al documento utilizzando la visualizzazione del modello dopo l'avvio di una nuova sessione effettuando l'accesso al sistema.

Modifica di un modello di documento

È possibile modificare nome, layout e contenuto di un modello utilizzando Gestione della conoscenza.

Per aggiornare un modello di documento

1. Dalla scheda Amministrazione accedere a Conoscenza, Documenti, Modelli documento.

   Appare il riquadro Elenco modelli documento.

2. Selezionare un nome di modello.

   Viene visualizzata la pagina Aggiorna modello documento.

3. Fare clic su Modifica dettagli.

   Viene visualizzato l'Editor HTML.

4. Modificare nome, contenuto o layout del modello. È possibile modificare i campi seguenti:

   Modello

   Consente di definire un nome univoco per il modello. Questo campo è obbligatorio.

   Dettagli

   Consente di visualizzare il contenuto statico dei documenti creati tramite il modello corrente. Se si seleziona l'opzione Origine HTML, è possibile modificare il codice HTML del corpo direttamente nel campo Corpo. Se si seleziona l'opzione Visualizzazione rapida, il campo Corpo risulta di sola lettura e visualizza il contenuto del corpo statico come compare al momento dell'esecuzione.

5. Fare clic su Modifica dettagli per specificare il contenuto statico e il layout di documenti che utilizzano il modello.

   Viene aperta la finestra dell'Editor HTML.

6. Modificare il codice utilizzando la barra degli strumenti per inserire tag segnaposto. Fare clic su OK.

   Il campo Dettagli mostra il contenuto aggiornato.

7. (Opzionale) Fare clic su Visualizzazione rapida.

   Il contenuto viene visualizzato come documento basato sul modello.

8. (Opzionale) Fare clic su Visualizzazione HTML.

   Il contenuto compare come codice HTML.

9. Fare clic su Salva.

   Viene visualizzata la pagina Dettagli modello documento.

10. Fare clic su Chiudi finestra.

    Nuovi documenti che usano il modello mostrano il nuovo contenuto e layout.

    Quando viene aggiornato l'elenco, appare il cambiamento al nome del modello.

Elencazione di modelli di documento

La pagina Elenco Modelli documento consente di creare e gestire modelli di documento, i quali specificano il contenuto e l'aspetto di documenti nell'archivio della conoscenza.

I seguenti modelli predefiniti vengono installati con il prodotto:

- Incorporato—Documento della conoscenza
- Incorporato—Struttura della conoscenza
- Incorporato—Modifica rapida

Il prodotto utilizza modelli predefiniti quando si creano documenti della conoscenza e documenti della struttura della conoscenza a meno che non si creino modelli di documento e si associno ai propri documenti.

Nota: in caso di installazione dell'opzione multi-tenancy, la pagina di elenco visualizzerà le impostazioni Titolare e Dati pubblici nel filtro di ricerca. L'opzione Dati pubblici può essere inclusa o esclusa per i dati del titolare: la ricerca viene eseguita unicamente per gli oggetti pubblici. Nelle pagine dei dettagli, selezionare il titolare appropriato dall'elenco. Se si seleziona <vuoto>, l'oggetto è pubblico.

Per elencare modelli di documento, selezionare Amministrazione, Conoscenza, Documenti, Modelli documento dalla scheda Amministrazione.

La pagina Elenco Modelli documento viene visualizzata e include le colonne seguenti:

Nome modello

Consente di elencare i modelli di documento correntemente definiti. Selezionare un nome di modello per aprire la finestra Aggiorna documento. Fare clic con il pulsante destro del mouse sul nome del modello per aprire il menu di scelta rapida Nome modello, che contiene i comandi per l'utilizzo del modello selezionato.

Predefinito

Visualizza un contrassegno che indica che un modello viene utilizzato come predefinito per i documenti appena creati oppure quando il modello di un documento specificato è stato eliminato. Per impostare un modello come impostazione predefinita, fare clic con il pulsante destro del mouse sul nome del modello e selezionare Imposta come predefinito dal menu di scelta rapida.

Nota: quando si crea un nuovo documento o si elimina un modello associato a un documento, il prodotto viene associato al modello predefinito (a meno che non venga selezionato un altro modello nella scheda Attributi della finestra Crea nuovo documento o Aggiorna documento di conoscenza).

In questa pagina sono disponibili i seguenti campi:

Modello

Consente di definire il nome del modello da ricercare. Questo campo viene visualizzato soltanto quando si fa clic su Mostra filtro.

Altri argomenti di ricerca

Consente di definire criteri di ricerca aggiuntivi. Questo campo viene visualizzato soltanto quando si fa clic sul collegamento Altro nel riquadro Ricerca conoscenza.

In questa pagina sono disponibili i seguenti pulsanti:

Cancella filtro

Consente di ripristinare i valori predefiniti di tutti i campi relativi al filtro del riquadro o della finestra.

Crea nuovo

Consente di aprire la finestra Crea nuovo modello documento per definire un nuovo modello di documento.

Cerca

Consente di avviare una ricerca per le voci che corrispondono ai criteri specificati. Quando non viene specificato alcun criterio, vengono visualizzati tutti gli elementi appropriati (ad esempio, cartelle/documenti, contatti, modelli, parole non significative o gruppi di autorizzazioni).

Mostra filtro/Nascondi filtro

Consente di mostrare o nascondere i campi con i quali è possibile filtrare una ricerca di elementi nella finestra, nel riquadro o nella finestra di dialogo corrente.

Nota: è possibile esportare i risultati sotto forma di elenco in Excel in modo che possano essere usati esternamente a CA SDM facendo clic sul pulsante Esporta nella pagina Elenco.

Filtrare l'Elenco Modelli documento

I modelli predefiniti vengono utilizzati quando si creano documenti della conoscenza e documenti della struttura della conoscenza, a meno che non vengano creati modelli di documenti e non vengano associati ai documenti. La pagina Elenco Modelli documento consente di creare e gestire modelli di documento, i quali specificano il contenuto e l'aspetto di documenti nell'archivio della conoscenza. È possibile filtrare modelli da questa pagina.

Per filtrare l'elenco modelli di documento

1. Fare clic sulla scheda Amministrazione.

   Viene visualizzata la pagina Amministrazione.

2. Fare clic su Conoscenza, Documenti, Modelli documento.

   Viene visualizzato l'Elenco Modelli documento.

3. Effettuare *una* delle operazioni seguenti:

   - Selezionare un modello dalla colonna Nome modello.

     Viene aperto il modello.

   - Effettuare la ricerca di un modello utilizzando la funzione di ricerca.

     Vengono visualizzati i risultati della ricerca del modello.

   - Selezionare Mostra filtro per filtrare la ricerca.

     La ricerca del modello verrà filtrata.

Aggiornamento dei modelli documento per la visualizzazione dei collegamenti delle relazioni

È possibile aggiornare i modelli di documenti della conoscenza di una versione precedente di CA SDM allo scopo di visualizzare le relazioni della conoscenza. È sufficiente modificare il modello aggiungendo i tag {TAG_PARENT} e {TAG_RELATED} per consentire ai documenti che utilizzano il modello di visualizzare le relazioni del documento, come i collegamenti padre-figlio e titolare.

Per modificare i modelli allo scopo di visualizzare le relazioni della conoscenza:

1. Aprire il modello documento della conoscenza.

   Viene visualizzata la pagina Aggiorna modello documento.

2. Fare clic su Modifica.
3. Selezionare la visualizzazione Fonte HTML.

   Nota: in alternativa, è possibile anche fare clic su Modifica dettagli per aprire l'editor HTML e aggiungere i tag {TAG_PARENT} e {TAG_RELATED}.

4. Selezionare *Selezione segnaposto modello* dal menu a discesa Modifica dettaglio per aggiungere tag al modello documento.

   I tag vengono aggiunti al modello.

5. Salvare e chiudere il modello.

   Il modello viene aggiornato in modo che visualizzi le relazioni della conoscenza.

Come creare collegamenti documento della conoscenza

È possibile aggiornare l'ambiente Gestione della conoscenza creando collegamenti documento. Le relazioni della conoscenza permettono di creare gerarchie di documenti e gestire le modifiche apportate ai documenti della conoscenza.

Per creare relazioni della conoscenza, effettuare le seguenti operazioni:

1. Definire i modelli di documenti della conoscenza per visualizzare o nascondere le relazioni padre-figlio in modalità di visualizzazione
2. Creare o modificare un documento della conoscenza

   Nota: per impostazione predefinita, è possibile aggiungere solo collegamenti a un documento della conoscenza non pubblicato. Se un documento è già stato pubblicato, aprire il documento in modalità modifica o rielaborazione per creare collegamenti documento. È possibile modificare le autorizzazioni dei documenti prima del processo di approvazione e dopo la pubblicazione.
3. È possibile creare uno *qualsiasi* dei seguenti collegamenti documento tramite la scheda Conoscenza correlata, in base alle esigenze del proprio ambiente Gestione della conoscenza:
   - Collegare il documento come Vedi anche non gerarchico

     È possibile collegare documenti della conoscenza ad altri documenti esistenti.
   - Collegare il documento come padre o figlio

     È possibile collegare documenti della conoscenza in relazioni padre-figlio.

     Nota: se si modifica un documento padre, viene visualizzato un avviso che indica che la modifica potrebbe avere affetto sui documenti figlio.
   - Collegare il documento globale a un documento assegnato a un titolare

     È possibile collegare documenti della conoscenza a un singolo titolare o a più titolari. È possibile ad esempio che un documento figlio abbia un titolare diverso rispetto al documento padre.

   La scheda Cronologia viene aggiornata al momento della creazione dei collegamenti documento per semplificare il controllo delle modifiche.
4. Salvare il documento e verificare che i collegamenti vengano visualizzati quando si apre il documento in Visualizzazione utente

   È possibile verificare che i collegamenti documento vengano visualizzati in base alle autorizzazioni definite.

Creazione di un collegamento Padre-Figlio

È possibile creare relazioni padre-figlio per i documenti della conoscenza. I collegamenti padre-figlio permettono di organizzare i documenti correlati per gli utenti del proprio ambiente.

Per creare un collegamento Padre-Figlio:

1. Creare un documento della conoscenza oppure aprire un documento in modalità modifica.

   Viene visualizzato il documento della conoscenza.

2. Scegliere la scheda della conoscenza relativa.

   Viene visualizzata la pagina Categorie.

   Nota: è anche possibile creare collegamenti dalla scheda Argomenti correlati. Usare i criteri di ricerca per trovare i documenti.

3. Individuare il documento che si desidera collegare nel riquadro Categorie (X).

   Fare clic con il pulsante destro del mouse nel riquadro Documenti e selezionare l'opzione *Collega come padre* o *Collega come figlio* per creare il collegamento tra i documenti.

   Viene creato il collegamento al documento.

Creazione di un collegamento Vedi anche

È possibile creare una relazione Vedi anche per i documenti della conoscenza del proprio ambiente. Le relazioni Vedi anche possono essere usate per gestire le gerarchie della conoscenza nel proprio ambiente.

Per creare un collegamento Vedi anche:

1. Creare un documento della conoscenza oppure aprire un documento in modalità rielaborazione.

   Viene visualizzato il documento della conoscenza.

2. Scegliere la scheda della conoscenza relativa.

   Viene visualizzata la pagina Categorie.

   Nota: è anche possibile creare collegamenti dalla scheda Argomenti correlati.

3. Individuare il documento che si desidera collegare nel riquadro Categorie (X).

   Fare clic con il pulsante destro del mouse sul documento nel riquadro Documenti e selezionare l'opzione *Collega documento come vedi anche*.

   Viene creato il collegamento al documento.

Rimozione dei collegamenti documento

È possibile rimuovere i collegamenti da un documento della conoscenza non pubblicato, come una relazione padre-figlio. Se il documento è già stato pubblicato, è necessario aprire il documento in modalità modifica o rielaborazione per rimuovere i collegamenti documento.

Per rimuovere un collegamento documento:

1. Aprire il documento della conoscenza.

   Viene visualizzato il documento.

2. Fare clic su Modifica.

   Viene visualizzata la pagina Aggiorna documento.

3. Scegliere la scheda della conoscenza relativa.

   Viene visualizzata la pagina Categorie.

4. Spostarsi nel riquadro Collegamenti documento.

5. Selezionare l'opzione *Rimuovi questo collegamento* dal menu contestuale per rimuovere il collegamento.

   I collegamenti documento vengono rimossi.

Categorie conoscenza

I documenti della conoscenza sono ordinati in *categorie della conoscenza*. Queste categorie possono essere gestite dai tecnici della conoscenza, dai gestori della conoscenza e dagli amministratori. Ciascuno di questi utenti utilizza Gestione della conoscenza per creare, copiare e modificare le categorie. Tuttavia, soltanto i gestori della conoscenza e gli amministratori possono eliminare le categorie. Quando si crea la struttura categoria in Categorie della conoscenza, di fatto si costruisce la struttura gerarchica che i dipendenti di Service Desk, i clienti e gli analisti utilizzano per accedere ai documenti a cui sono interessati.

Assegnare ciascun documento a una categoria primaria. Ad esempio, qualsiasi conoscenza correlata a Microsoft Word deve essere aggiunta alla categoria di Microsoft Word. In aggiunta, Gestione della conoscenza consente di associare un documento a più categorie secondarie e ad altri documenti. In questo modo, un documento può essere classificato in diverse categorie applicabili e può fornire risultati di ricerca più corretti.

La struttura di categoria ha le seguenti funzioni:

- Organizza le soluzioni della conoscenza in gruppi gestibili
- Rende più semplice l'assegnazione di diritti di accesso

- Consente di ricercare le soluzioni con FAQ/Sfoglia

  Per usare la funzionalità di esplorazione delle categorie da un Incidente, è necessario verificare che l'area Incidente e la categoria della conoscenza corrispondano. Quando si crea un Incidente basato su un documento della conoscenza, l'are Incidente viene impostata dalla categoria del documento. Quindi, la categoria e l'area corrispondono sempre.

- Crea un collegamento documento—Quando si visualizza uno dei due documenti, viene visualizzato il collegamento *Vedi anche*. Il collegamento *Vedi anche* consente di passare direttamente da un documento collegato a un altro.

Creazione di una categoria di conoscenza

Per ogni categoria è possibile definire le proprietà che identificano gli attributi o le qualità da associare al ticket e creare un flusso di lavoro che identifica tutte le singole attività necessarie all'adempimento del ticket.

È possibile utilizzare categorie per specificare valori predefiniti per certi campi in ticket, oppure associare automaticamente un livello di servizio a ticket assegnando un tipo di servizio predefinito a categorie. Ogniqualvolta in cui un analista assegna una categoria a un ticket, tutte le informazioni associate alla categoria vengono automaticamente associate al ticket.

Nota: se si utilizza Multi-tenancy, viene visualizzato un elenco a discesa Titolare nel filtro di ricerca del documento della conoscenza. Se si seleziona <vuoto> in questo elenco a discesa, la ricerca è pubblica. Nella pagina elenco è visualizzata anche una colonna relativa al titolare.

Per creare una categoria:

1. Dalla scheda Amministrazione accedere a Conoscenza, Categorie della conoscenza.

   Viene visualizzata la pagina Categorie della conoscenza.

2. Fare clic con il pulsante destro del mouse sulla categoria in cui si desidera creare la categoria. Selezionare Nuova categoria dal menu di scelta rapida.

   Viene aperta la finestra Crea Nuova categoria.

3. Compilare i campi (a pagina 1012) in modo appropriato.

4. Fare clic su Autorizzazioni.

   Viene visualizzata la scheda Autorizzazioni.

5. Selezionare una delle seguenti opzioni di autorizzazioni per la categoria:

   Eredita da padre

   Consente di specificare che la nuova categoria ha le stesse impostazioni di autorizzazione della sua categoria padre.

Nota: l'opzione Eredita da padre non è disponibile se si sceglie la categoria IN ALTO prima di aprire la pagina di creazione della categoria.

Controllo per Gruppo

Specifica autorizzazioni di categoria per assegnare ai gruppi accesso di lettura o scrittura alla categoria.

Controllo per Ruolo

Specifica autorizzazioni di categoria per assegnare ai ruoli accesso di lettura o scrittura alla categoria.

Nota: se si modificano i controlli, come nel caso della modifica delle autorizzazioni di categoria da gruppo a ruolo, verrà visualizzato un avviso che indica che le autorizzazioni precedenti vengono eliminate per quella categoria.

Concedi autorizzazione in scrittura a tutti

Specifica che tutti gli utenti hanno accesso di scrittura alla categoria. L'accesso di scrittura indica che è possibile modificare o eliminare questa categoria.

Nota: se si seleziona la casella di controllo Concedi autorizzazione in scrittura a tutti, viene selezionata automaticamente la casella di controllo Concedi autorizzazione in lettura a tutti.

Concedi autorizzazione in lettura a tutti

Specifica che tutti gli utenti hanno accesso di lettura alla categoria. Le autorizzazioni di lettura indicano che è possibile visualizzare la categoria, ma che non è possibile modificarla o eliminarla. Gli utenti con diritti di amministratore possono modificare una cartella anche se il gruppo con autorizzazione loro associato non può farlo. Se un utente appartiene a più gruppi di autorizzazione con diversi livelli di accesso alla categoria, l'utente ottiene il livello di accesso più alto disponibile (ad esempio, se un gruppo dispone di accesso di sola lettura e un altro dispone di accesso di scrittura, l'utente otterrà accesso di scrittura).

Nota: se si seleziona la casella di controllo Concedi autorizzazione in scrittura a tutti, viene selezionata automaticamente la casella di controllo Concedi autorizzazione in lettura a tutti.

Importante: quando si concedono autorizzazioni per Tutti, l'accesso per ruolo o gruppo è lo stesso. Se è stato selezionato Tutti e Controllo per Ruolo, dopo il salvataggio delle autorizzazioni, risulterà selezionato Controllo per Gruppo.

6. (Opzionale) Specificare le autorizzazioni di lettura-scrittura per i gruppi o ruoli specifici tramite gli elenchi Disponibile e selezionato.

   Si utilizza questa opzione per gestire quali gruppi o ruoli dispongono di accesso di lettura o scrittura per la categoria. È possibile scegliere uno o più gruppi o ruoli di autorizzazione dall'elenco Gruppi/Ruoli disponibili, quindi utilizzare i pulsanti Aggiungi e Rimuovi per spostare i gruppi o i ruoli selezionati negli elenchi di Gruppi/Ruoli con Autorizzazioni in scrittura e Gruppi/Ruoli con Autorizzazioni in lettura.

7. Fare clic su Salva.

   Viene visualizzata la pagina Dettagli categoria.

8. Fare clic su Chiudi finestra.

   Il riquadro Categorie della conoscenza viene aggiornato per includere la nuova categoria.

Ulteriori informazioni:

Campi di categoria (a pagina 1012)

Campi di categoria

Titolo

Nome della categoria.

Descrizione

Descrizione della categoria.

Proprietario categoria

Indica la persona responsabile della categoria. Se un contatto è definito come proprietario di una categoria, dispone di un collegamento nella scheda Report della conoscenza denominato "Categorie personali" mediante il quale può visualizzare le statistiche per tale categoria e i documenti in essa contenuti. Questa persona è anche il proprietario predefinito dei nuovi documenti creati nella categoria se l'utente che li crea non è un analista oppure se l'analista seleziona 'Assegna a proprietario categoria' al momento della creazione dei documenti.

Modello documenti

Consente di specificare il modello di documento che deve essere usato per tutti i documenti associati alla categoria. L'opzione <vuoto> indica che non è stato definito alcun modello ma che per impostazione predefinita verrà utilizzato quello incorporato.

Modello processo di approvazione

Consente di specifica il modello predefinito da usare per il processo di approvazione di tutti i documenti associati alla categoria. Il modello del processo di approvazione definisce le fasi del flusso di lavoro che devono precedere la pubblicazione di un documento. L'impostazione predefinita <vuoto> indica che verrà utilizzato il modello predefinito dell'applicazione.

Consenti la creazione di forum in questa categoria

Indica se gli analisti sono autorizzati o meno a creare forum nella categoria.

Aree Richiesta/Incidente/Problema

Indica un'area Richiesta/Incidente/Problema impostata dall'amministratore per designare l'area di responsabilità. È possibile fare clic sull'icona di ricerca per effettuare la scelta dalle aree disponibili.

Categoria questione

Indica una categoria questione definita dall'amministratore per designare un'area di responsabilità. È possibile fare clic sull'icona di ricerca per effettuare la scelta dalle aree disponibili.

Modifica di una categoria

È possibile modificare una categoria nell'ambiente Gestione della conoscenza. Le categorie determinano il contenuto degli ordini di cambiamento e delle questioni dopo che sono stati creati. Per ogni categoria è possibile definire le proprietà che identificano gli attributi o le qualità da associare al ticket e creare un flusso di lavoro che identifica tutte le singole attività necessarie all'adempimento del ticket.

È possibile utilizzare categorie per specificare valori predefiniti per certi campi in ticket, oppure associare automaticamente un livello di servizio a ticket assegnando un tipo di servizio predefinito a categorie. Ogniqualvolta in cui un analista assegna una categoria a un ticket, tutte le informazioni associate alla categoria vengono automaticamente associate al ticket.

Per modificare una categoria:

1. Dalla scheda Amministrazione accedere a Conoscenza, Categorie della conoscenza.

   Viene visualizzata la pagina Categorie della conoscenza.

2. Fare clic con il pulsante destro del mouse sulla categoria da modificare, quindi selezionare Modifica dal menu di scelta rapida.

   Viene aperta la scheda Contenuto della pagina Aggiorna categoria.

   Nota: non è possibile eliminare o modificare la categoria In alto.

3. Aggiornare uno o più campi (a pagina 1012) secondo necessità.

4. Fare clic su Autorizzazioni.

   Viene visualizzata la scheda Autorizzazioni.

5. Selezionare una delle seguenti opzioni di autorizzazioni per la categoria:

   Eredita da padre

   Consente di specificare che la nuova categoria ha le stesse impostazioni di autorizzazione della sua categoria padre.

   Nota: l'opzione Eredita da padre non è disponibile se si sceglie la categoria IN ALTO prima di aprire la pagina di creazione della categoria.

   Controllo per Gruppo

   Specifica autorizzazioni di categoria per assegnare ai gruppi accesso di lettura o scrittura alla categoria.

   Controllo per Ruolo

   Specifica autorizzazioni di categoria per assegnare ai ruoli accesso di lettura o scrittura alla categoria. Se si seleziona Tutti e Controllo per Ruolo, dopo il salvataggio delle autorizzazioni, risulterà selezionato Controllo per Gruppo.

   Nota: se si modificano i controlli, come nel caso della modifica delle autorizzazioni di categoria da gruppo a ruolo, verrà visualizzato un avviso che indica che le autorizzazioni precedenti vengono eliminate per quella categoria.

6. (Opzionale) Specificare le autorizzazioni di lettura-scrittura per la categoria.

   Si utilizza questa opzione per gestire quali gruppi o ruoli dispongono di accesso di lettura o scrittura per la categoria. Quando si seleziona questa opzione, la finestra si aggiorna per includere le caselle di controllo (a pagina 1017) Concedi autorizzazione in scrittura a tutti e Concedi autorizzazione in lettura a tutti.

7. Fare clic su Salva.

   La categoria modificata viene visualizzata nella pagina Elenco categorie della conoscenza.

Eliminazione di una categoria

È possibile rimuovere una categoria dalla struttura Categoria della conoscenza. Quando si elimina una categoria, è possibile specificare se devono essere rimosse o meno le sottocategorie della categoria selezionata e tutti i collegamenti documento associati.

Nota: Questa funzione è disponibile solo per amministratori di sistema e gestori della conoscenza.

Per eliminare una categoria:

1. Dalla scheda Amministrazione accedere a Conoscenza, Categorie della conoscenza.

   Viene visualizzata la pagina Categorie della conoscenza.

2. Fare clic con il pulsante destro del mouse sulla categoria da eliminare, quindi selezionare Elimina categoria dal menu di scelta rapida.

   Viene visualizzata la pagina Elimina categoria.

   Nota: non è possibile eliminare o modificare la categoria In alto.

3. (Opzionale) Eseguire *una* delle seguenti operazioni:

   - Selezionare la casella di controllo Includi sottocategorie per eliminare tutte le sottocategorie della categoria selezionata.
   - Deselezionare la casella di controllo Includi sottocategorie per spostare tutte le sottocategorie dalla categoria selezionata alla più vicina categoria padre disponibile.

4. (Opzionale) Eseguire *una* delle seguenti operazioni:

   - Selezionare la casella di controllo Includi documenti per eliminare i documenti contenuti nella categoria selezionata. Quando si seleziona la casella di controllo Includi documenti, vengono visualizzate le seguenti opzioni:
     - **Elimina solo documenti collegati alla categoria primaria** - Elimina solo i documenti per i quali la categoria selezionata è identificata nel riquadro Categorie della conoscenza come categoria principale del documento.
     - **Elimina tutti i documenti collegati alla categoria —**Elimina tutti i documenti contenuti nella categoria selezionata.
   - Selezionare la casella di controllo Includi documenti per spostare i documenti dalla categoria selezionata alla più vicina categoria padre disponibile.

   Fare clic su OK.

   Il prodotto elimina la categoria selezionata e il riquadro Categoria della conoscenza viene aggiornato.

Spostamento di una categoria

È possibile spostare una categoria, le sue sottocategorie e tutti i collegamenti documento associati dall'ubicazione corrente in un'altra categoria.

Nota: questa funzionalità è disponibile solo se Gestione della conoscenza è installato.

Per tagliare e incollare una categoria:

1. Dalla scheda Amministrazione accedere a Conoscenza, Categorie della conoscenza.

   Viene visualizzata la pagina Categorie della conoscenza.

2. Fare clic con il pulsante destro del mouse sulla categoria da spostare, quindi selezionare Taglia categoria dal menu di scelta rapida.

   La categoria selezionata, le sottocategorie e tutti i collegamenti documento associati vengono inseriti in memoria.

3. Fare clic con il pulsante destro del mouse sulla categoria in cui incollare le informazioni tagliate, quindi selezionare Incolla categoria dal menu di scelta rapida.

   La categoria tagliata viene spostata dalla sua ubicazione originale a sotto la categoria selezionata. Il riquadro Categorie della conoscenza viene aggiornato per visualizzare la nuova struttura di categoria.

Copia di una categoria con collegamenti documento

È possibile inserire una copia della categoria, delle sue sottocategorie e di tutti i collegamenti documento associati in un'altra categoria senza rimuovere la selezione dall'ubicazione originale.

Per copiare e incollare una categoria con collegamenti documento:

1. Dalla scheda Amministrazione accedere a Conoscenza, Categorie della conoscenza.

   Viene visualizzata la pagina Categorie della conoscenza.

2. Fare clic con il pulsante destro del mouse sulla categoria da copiare e selezionare Copia categoria con collegamenti documento dal menu di scelta rapida.

   La categoria selezionata, le sottocategorie e tutti i collegamenti documento associati vengono inseriti in memoria.

3. Fare clic con il pulsante destro del mouse sulla categoria in cui incollare le informazioni copiate, quindi scegliere Incolla categoria dal menu di scelta rapida.

   Le informazioni copiate compaiono sotto la categoria selezionata. Il riquadro Categorie della conoscenza viene aggiornato per visualizzare la nuova struttura di categoria.

Copia di una categoria senza collegamenti documento

È possibile inserire una copia della categoria e delle sue sottocategorie in un'altra sottocategoria senza rimuovere la selezione dall'ubicazione originale oppure copiare i collegamenti documento associati.

Per copiare e incollare una categoria senza collegamenti documento:

1. Dalla scheda Amministrazione accedere a Conoscenza, Categorie della conoscenza.

   Viene visualizzata la pagina Categorie della conoscenza.

2. Fare clic con il pulsante destro del mouse sulla categoria da copiare, quindi selezionare Copia categoria dal menu di scelta rapida.

   La categoria selezionata e le sottocategorie vengono inserite in memoria.

3. Fare clic con il pulsante destro del mouse sulla categoria in cui incollare le informazioni copiate, quindi scegliere Incolla categoria dal menu di scelta rapida.

   Le informazioni copiate compaiono sotto la categoria selezionata. Il riquadro Categorie della conoscenza viene aggiornato per visualizzare la nuova struttura di categoria.

Gestione delle autorizzazioni categoria

È possibile gestire le autorizzazioni relative alle categorie dell'ambiente Gestione della conoscenza concedendo specifiche autorizzazioni in lettura/scrittura in base al gruppo o al ruolo È possibile specificare chi può visualizzare, modificare, eliminare o aggiungere sottocategorie a una categoria.

Nota: è possibile utilizzare autorizzazioni in scrittura vuote per documenti e categorie. Se non si selezionano autorizzazioni in scrittura, vengono impostate autorizzazioni in scrittura vuote. Solo gli utenti con privilegi possono modificare categorie e documenti con autorizzazioni in scrittura vuote.

Per gestire le autorizzazioni categoria

1. Nella scheda Amministrazione, accedere a Conoscenza, Categorie della conoscenza.

   Viene visualizzata la pagina Categorie della conoscenza.

2. Fare clic con il pulsante destro del mouse sulla categoria al di sotto della quale si desidera creare la categoria e selezionare Nuova categoria dal menu di scelta rapida per gestire le autorizzazioni di una nuova categoria.

   Nella pagina Crea nuova categoria viene visualizzata la scheda Contenuto.

3. Fare clic su Autorizzazioni.

   Viene visualizzata la scheda Autorizzazioni.

4. Selezionare una delle seguenti opzioni di autorizzazioni per la categoria:

   Eredita da padre

   Consente di specificare che la nuova categoria ha le stesse impostazioni di autorizzazione della sua categoria padre.

   Nota: se si seleziona la categoria In alto prima di aprire la pagina Crea nuova categoria, l'opzione Eredita da padre non è disponibile.

Controllo per Gruppo

Specifica autorizzazioni di categoria per assegnare ai gruppi accesso di lettura o scrittura alla categoria.

Controllo per Ruolo

Specifica autorizzazioni di categoria per assegnare ai ruoli accesso di lettura o scrittura alla categoria.

Nota: se si modificano i controlli, ad esempio modificando le autorizzazioni di categoria da gruppo a ruolo, viene visualizzato un avviso che indica che le autorizzazioni precedenti vengono eliminate.

Concedi autorizzazione in scrittura a tutti

Specifica che tutti gli utenti hanno accesso di scrittura alla categoria. L'accesso di scrittura indica che è possibile modificare o eliminare questa categoria.

Nota: se si seleziona la casella di controllo Concedi autorizzazione in scrittura a tutti, viene selezionata automaticamente la casella di controllo Concedi autorizzazione in lettura a tutti.

Concedi autorizzazione in lettura a tutti

Specifica che tutti gli utenti hanno accesso di lettura alla categoria. Le autorizzazioni di lettura indicano che è possibile visualizzare la categoria, ma che non è possibile modificarla o eliminarla. Gli utenti con diritti di amministratore possono modificare una cartella anche se il gruppo con autorizzazione loro associato non può farlo. Se un utente appartiene a più gruppi di autorizzazione con diversi livelli di accesso alla categoria, l'utente ottiene il livello di accesso più alto disponibile (ad esempio, se un gruppo dispone di accesso di sola lettura e un altro dispone di accesso di scrittura, l'utente otterrà accesso di scrittura).

Nota: se si seleziona la casella di controllo Concedi autorizzazione in scrittura a tutti, viene selezionata automaticamente la casella di controllo Concedi autorizzazione in lettura a tutti.

Importante: quando si concedono autorizzazioni per Tutti, l'accesso per ruolo o gruppo è lo stesso. Se è stato selezionato Tutti e Controllo per Ruolo, dopo il salvataggio delle autorizzazioni, risulterà selezionato Controllo per Gruppo.

5. Concedere la autorizzazioni in lettura/scrittura appropriate a gruppi o ruoli specifici selezionandoli dagli elenchi Disponibile e Selezionato.

   È possibile scegliere uno o più gruppi o ruoli di autorizzazione dall'elenco Gruppi/Ruoli disponibili, quindi utilizzare i pulsanti Aggiungi e Rimuovi per spostare i gruppi o i ruoli selezionati negli elenchi di Gruppi/Ruoli con Autorizzazioni in scrittura e Gruppi/Ruoli con Autorizzazioni in lettura.

   Nota: tutti i gruppi o ruoli aggiunti all'elenco delle autorizzazioni vengono automaticamente aggiunti all'elenco delle autorizzazioni in lettura. Quando si seleziona la casella di controllo Concedi autorizzazioni in lettura a tutti, non è necessario aggiungere gruppi o ruoli all'elenco delle autorizzazioni in lettura.

6. Fare clic su Salva.

   Viene visualizzata la pagina Dettagli categoria.

7. Fare clic su Chiudi finestra.

   La categoria modificata viene visualizzata nel riquadro Categorie della conoscenza.

Report e metriche

È possibile controllare l'efficienza dell'archivio della conoscenza utilizzando i vari strumenti di reporting.

- Knowledge Report Card
- Report basati sul Web predefiniti per Gestione della conoscenza
- Moduli Web basati su ruoli

Questi strumenti consentono di visualizzare statistiche sull'utilità dei documenti e sulla relativa efficacia di risolvere problemi.

Ulteriori informazioni:

Knowledge Report Card (a pagina 1019)
Report basati sul Web (a pagina 1021)
Moduli Web report basati sul ruolo (a pagina 1021)

Knowledge Report Card

La scheda Report della conoscenza visualizza informazioni sul contributo fornito alla conoscenza da ciascun utente finale e fornisce feedback su quali documenti della conoscenza sono più efficaci. È possibile usare queste informazioni per migliorare il processo di creazione dei documenti della conoscenza e fornire il migliore supporto possibile agli utenti finali del proprio ambiente.

Definizione delle statistiche relative alla scheda report della conoscenza

Utilizzare la pagina Scheda report della conoscenza per definire la pianificazione in base alla quale calcolare e inviare le notifiche relative alla Scheda report della conoscenza e per definire il contenuto delle notifiche tramite posta elettronica della Scheda report della conoscenza.

Nota: le versioni di rielaborazione e i documenti ritirati non vengono presentati quando viene eseguito il calcolo scheda Report della conoscenza.

Per definire statistiche relative alla scheda Report della conoscenza:

1. Nella scheda Amministrazione, selezionare Conoscenza, Scheda report della conoscenza.

   La pagina Scheda report si apre.

2. Completare i campi seguenti in modo appropriato.

   Ultimo aggiornamento

   Esegue il calcolo del servizio Scheda report.

   Impostazione predefinita: disattivato

   Nota: se non viene eseguito il calcolo, non vengono raccolte le statistiche per presentare i dati e si seleziona il comando Scheda report della conoscenza nel menu Visualizza nella scheda Conoscenza, viene visualizzato il messaggio: "Eseguire calcolo scheda report".

   Pianifica

   Pianifica la Scheda Report.

   - **Il calcolo del servizio Scheda report verrà eseguito il xxx e verrà eseguito ogni xxx** -- Consente di specificare la frequenza con la quale viene eseguito il ricalcolo delle statistiche della Scheda report.
   - **Le notifiche tramite posta elettronica del servizio Scheda report verranno inviate il xxx e ogni xxx** -- Consente di specificare la frequenza alla quale inviare le notifiche della Scheda Report.

     Impostazione predefinita: mai
   - **La scheda report Posta elettronica dovrebbe visualizzare le statistiche per i precedenti xxx—**Specifica il numero di volte in cui la notifica della Scheda report contiene informazioni. Questo campo è disponibile solo quando si seleziona un valore diverso da Mai nell'elenco Le notifiche di posta elettronica del servizio Scheda report verranno eseguite ogni xxx.

     Impostazione predefinita: 365 giorni

3. Fare clic su Salva.

   Vengono definite le statistiche della scheda Report della conoscenza.

Report basati sul Web

CA Business Intelligence installa un set di report predefiniti Gestione della conoscenza. Questi report sono distribuiti automaticamente in CA Business Intelligence dopo l'installazione di CA SDM.

I report vengono sviluppati con BusinessObjects Web Intelligence o con Crystal Reports. Gli utenti autorizzati possono visualizzare i report nella scheda Report di CA SDM.

Moduli Web report basati sul ruolo

È possibile specificare i moduli Web dei report che devono essere visualizzati quando un gestore o analista autorizzato seleziona l'icona Elenco Report nella scheda Report.

I moduli Web report sono gestiti attraverso l'elenco ruoli nella seguente posizione: Amministrazione, Gestione ruoli e protezione, Gestione ruoli.

Cerca

La funzionalità Cerca permette agli amministratori di effettuare le seguenti attività:

- Gestire il motore di ricerca Gestione della conoscenza e definire le impostazioni da usare per la gestione delle parole indesiderate, i termini speciali e i sinonimi esclusi o inclusi nelle ricerche
- Definire le impostazioni da usare per l'analisi dei documenti
- Definire le impostazioni di ricerca predefinite
- Creare i "documenti consigliati" da visualizzare nei risultati delle ricerche L'opzione Elenco FAQ dinamico viene utilizzata per inviare i documenti consigliati agli utenti.

  Nota: un documento può disporre di diverse autorizzazioni rispetto agli allegati collegati al documento.

Ulteriori informazioni:

Motore di ricerca SC (a pagina 1022)
Documenti consigliati (a pagina 1033)
Impostazione delle impostazioni di ricerca predefinite (a pagina 1037)
Opzioni integrazione CA SDM (a pagina 1038)

Motore di ricerca SC

Al termine dell'installazione di CA SDM, il motore di ricerca SC viene configurato come motore di ricerca predefinito. Le ricerche dell'archivio della conoscenza sono limitate ai documenti della conoscenza. Il motore di ricerca viene configurato tramite la scheda Amministrazione, Conoscenza, Cerca, nodo Motore di ricerca SC.

Il nodo Motore di ricerca SC consente la gestione delle seguenti opzioni:

- Parole di disturbo
- Termini speciali
- Sinonimi

Ulteriori informazioni:

Utilizzo del motore di ricerca Gestione della conoscenza (a pagina 1022)

Utilizzo del motore di ricerca Gestione della conoscenza

Al termine dell'installazione di CA SDM, il motore di ricerca Gestione della conoscenza viene configurato come motore di ricerca predefinito. Le ricerche dell'archivio della conoscenza sono limitate ai documenti della conoscenza.

È possibile specificare l'accesso facilitato e le impostazioni predefinite per tutte le fonti della conoscenza utilizzando un ruolo utente. Per impostazione predefinita, le ricerche nei documenti della conoscenza possono essere effettuate da tutti i ruoli utente.

Procedere come descritto di seguito:

1. Fare clic sulla scheda Amministrazione.

   Viene visualizzata la console di amministrazione.

2. Fare clic su Gestione opzioni, Motore di ricerca.

   Viene visualizzato l'Elenco opzioni.

3. Fare clic su ebr_version.

   Viene visualizzata la pagina Dettagli opzioni.

   Fare clic su Modifica. Viene visualizzata la pagina Aggiorna opzioni.

4. Selezionare il motore di ricerca KT.
5. Fare clic su Salva, Aggiorna.

   La pagina Dettagli opzioni viene aggiornata con la propria selezione.

6. Fare clic su Chiudi finestra.
7. Riavviare i servizi CA SDM.

Ulteriori informazioni:

Parole non significative, sinonimi e termini speciali (a pagina 1023)
Creare parole non significative (a pagina 1024)
Modifica di parole non significative (a pagina 1025)
Visualizzazione di parole non significative (a pagina 1025)
Creazione di un termine speciale (a pagina 1026)
Modifica di un termine speciale (a pagina 1026)
Visualizzazione di termini speciali (a pagina 1027)
Creazione di un sinonimo (a pagina 1028)
Visualizzazione di sinonimi (a pagina 1028)
Modifica di un sinonimo (a pagina 1029)
Impostazioni di analisi (a pagina 1029)

Parole non significative, sinonimi e termini speciali

È possibile definire parole (sinonimi, parole non significative e termini speciali) per le ricerche in linguaggio naturale e di parole chiave eseguite in CA SDM. L'aggiunta o l'eliminazione dei seguenti termini influisce significativamente sui risultati delle ricerche restituiti all'utente:

Parole non significative

Consente di specificare le parole che non apportano alcun contributo al processo di ricerca e possono pertanto essere ignorate. Ad esempio, le preposizioni e gli articoli spesso vengono definiti come parole non significative. Utilizzare la pagina Elenco parole non significative per specificare le parole che il prodotto può ignorare in documenti e query senza conseguenze sui risultati di ricerca.

Termini speciali

Consente di specificare un termine che deve essere considerato come una parola singola durante il processo di ricerca. Il termine può essere costituito da più parole o contenere caratteri speciali. Ad esempio, è possibile aggiungere come termini speciali le parole che contengono un carattere non alfanumerico, come la barra (/) in TCP/IP, il trattino (-) in Mario-Rossi oppure il carattere di sottolineatura in SERVER_LOCALE. Nella propria valutazione di quali parole definire come termini speciali, prendere in considerazione parole valide che potrebbero essere divise durante il processo di ricerca perché contengono un carattere non alfanumerico.

Sinonimi

Consente di specificare una parola che ha lo stesso significato di un'altra parola. È possibile aggiungere sinonimi per permettere all'utente di trovare informazioni quando ricerca una parola specifica, se esiste un sinonimo se esiste un sinonimo nell'archivio della conoscenza. È possibile anche definire più sinonimi per la stessa parola. Il sistema crea automaticamente contrari utilizzando le parole chiave definite. Ad esempio, se si specifica computer come sinonimo della parola PC, PC diventa automaticamente un sinonimo della parola computer. Utilizzare la pagina Elenco Sinonimi per specificare coppie di parole chiave/sinonimi che il prodotto utilizza in modo intercambiabile durante l'analisi di documenti e query. Le coppie di parole chiave e sinonimi consentono di migliorare i risultati di ricerca.

Nota: una volta create, modificate o eliminate parole non significative, termini speciali, sinonimi o impostazioni di analisi, utilizzare l'utilità di reindicizzzazione della conoscenza fornita con il prodotto per reindicizzare l'archivio della conoscenza.

Creare parole non significative

La finestra Crea Nuova parola non significativa consente di aggiungere una nuova parola all'elenco di parole che il prodotto può ignorare nei documenti e nelle query senza compromettere i risultati di ricerca.

Per creare una parola non significativa:

1. Nella scheda Amministrazione, selezionare Conoscenza, Cerca, Motore di ricerca SC, Parole non significative.

   Viene visualizzata la pagina Elenco Parole non significative.

2. Fare clic su Crea nuovo.

3. Viene visualizzata la pagina Crea Nuova parola non significativa.

4. Immettere la parola da definire come parola non significativa nel campo Parola non significativa.

   Nota: non è possibile definire una parola non significativa esistente come sinonimo o parola chiave.

5. Fare clic su Salva

   La nuova parola non significativa viene visualizzata nella pagina Elenco Parole non significative. Per aggiornare la nuova parola non significativa, è possibile fare clic sul pulsante Modifica.

Nota: una volta create, modificate o eliminate parole non significative, termini speciali, sinonimi o impostazioni di analisi, utilizzare l'utilità di reindicizzzazione della conoscenza fornita con il prodotto per reindicizzare l'archivio della conoscenza.

Modifica di parole non significative

È possibile modificare una parola non significativa già creata nella pagina Elenco Parole non significative.

Nota: una volta create, modificate o eliminate parole non significative, termini speciali, sinonimi o impostazioni di analisi, utilizzare l'utilità di reindicizzazione della conoscenza fornita con il prodotto per reindicizzare l'archivio della conoscenza.

Per modificare una parola non significativa:

1. Fare clic con il pulsante destro del mouse sulla parola non significativa desiderata nell'elenco Parole non significative e selezionare Proprietà dal menu di scelta rapida.

   Viene visualizzata la pagina Aggiorna parola non significativa.

2. Immettere le modifiche desiderate nel campo Parola non significativa.

   Nota: non è possibile definire una parola non significativa esistente come sinonimo o parola chiave.

3. Fare clic su Salva.

   La nuova parola non significativa viene visualizzata nella pagina Elenco Parole non significative.

Nota: una volta create, modificate o eliminate parole non significative, termini speciali, sinonimi o impostazioni di analisi, utilizzare l'utilità di reindicizzazione della conoscenza fornita con il prodotto per reindicizzare l'archivio della conoscenza.

Visualizzazione di parole non significative

È possibile visualizzare informazioni di riepilogo per ciascuna parola non significativa memorizzata nella pagina Elenco Parole non significative.

Per visualizzare le informazioni di riepilogo per ciascuna parola non significativa, selezionare la scheda Amministrazione, Conoscenza, Cerca, Motore di ricerca SC, Parole non significative.

Viene visualizzata la pagina Elenco Parole non significative che mostra i seguenti campi:

Parola non significativa

Consente di definire la parola non significativa da cercare. Questo campo viene visualizzato soltanto quando si fa clic su Mostra filtro.

Altri argomenti di ricerca

Consente di definire criteri di ricerca aggiuntivi. Questo campo viene visualizzato soltanto quando si fa clic sul collegamento Altro nella pagina Ricerca della conoscenza.

Elenco Parole non significative

Consente di visualizzare le parole da filtrare nelle richieste di ricerca. L'elenco viene visualizzato quando si fa clic sul pulsante Ricerca. Se si inserisce una parola nella casella Parola non significativa, l'elenco visualizzerà unicamente la parola specificata. Se la casella Parola non significativa viene lasciata vuota, nell'elenco vengono visualizzate tutte le parole non significative definite per il prodotto.

Dalla pagina Elenco Parole non significative, è possibile effettuare le seguenti attività:

- Creare parole non significative (a pagina 1024)
- Modifica di parole non significative (a pagina 1025)

Creazione di un termine speciale

È possibile usare la pagina Crea Nuovo termine speciale per specificare una parola o frase che il prodotto deve considerare equivalente a singole parole chiave durante l'analisi di documenti e query.

Per creare un termine speciale:

1. Nella scheda Amministrazione, accedere a Conoscenza, Cerca, Motore di ricerca SC, Termini speciali.

   Viene visualizzata la pagina Elenco Termini speciali.

2. Fare clic su Crea nuovo.

   Viene visualizzata la pagina Crea Nuovo termine speciale.

3. Immettere la parola o frase che si desidera definire come termine speciale nel campo Termine speciale.

4. Fare clic su Salva.

   La finestra Crea Nuovo termine speciale si chiude e viene visualizzata la finestra Dettagli termine speciale che consente di verificare la parola o frase aggiunta. È possibile usare il pulsante Modifica per aggiornare il nuovo termine. Il termine aggiornato viene visualizzato nella pagina Elenco Termini speciali.

Modifica di un termine speciale

È possibile modificare un termine speciale.

Per modificare un termine speciale:

1. Fare clic con il pulsante destro del mouse sul termine da modificare e selezionare Modifica dal menu di scelta rapida.

   Viene visualizzata la pagina Aggiorna termine speciale.

2. Immettere la parola o frase che si desidera definire come termine speciale nel campo Termine speciale.
3. Fare clic su Salva.

   La finestra Aggiorna termine speciale si chiude e viene visualizzata la finestra Dettagli termine speciale che consente di verificare la parola o frase aggiunta. Il termine aggiornato viene visualizzato nella pagina Elenco termini speciali.

Visualizzazione di termini speciali

È possibile visualizzare le informazioni di riepilogo per ciascun termine speciale.

Per visualizzare i termini speciali, selezionare la scheda Amministrazione e successivamente Conoscenza, Cerca, Motore di ricerca SC, Termini speciali.

Viene visualizzata la pagina Elenco Termini speciali ed è possibile usare i seguenti campi per modificare i termini predefiniti da visualizzare oppure creare termini speciali personalizzati:

Termine speciale

Consente di definire un termine speciale da ricercare. Questo campo viene visualizzato soltanto quando si fa clic su Mostra filtro.

Altri argomenti di ricerca

Consente di definire criteri di ricerca aggiuntivi. Questo campo viene visualizzato soltanto quando si fa clic sul collegamento Altro nel riquadro Ricerca conoscenza.

Termini speciali

Consente di visualizzare le parole o le frasi contenenti spazi o caratteri (ad esempio trattini, barre, ecc) che il prodotto deve considerare come singole parole chiave durante l'analisi delle query. Se si inserisce una parola nella casella Termine speciale prima di fare clic su Ricerca, nell'elenco viene visualizzata solo la parola specificata. Se la casella Termine speciale viene lasciata vuota, nell'elenco vengono visualizzati tutti i termini speciali definiti per il prodotto.

Dalla pagina Elenco Termini speciali, è possibile effettuare le seguenti attività:

- Creazione di un termine speciale (a pagina 1026)
- Modifica di un termine speciale (a pagina 1026)

Creazione di un sinonimo

I sinonimi sono parole o frasi che hanno un significato identico o simile alla parola chiave a cui sono associati.

Se si definisce un nuovo sinonimo complesso (un sinonimo contenente più parole separate da spazi o altri delimitatori), è necessario anche creare un termine speciale identico per consentire al prodotto di considerare il sinonimo come entità singola. Se ad esempio si definisce "Computer Associates" come sinonimo di "CA", è necessario anche definire "Computer Associates" come termine speciale.

Nota: non è possibile definire un sinonimo o parola chiave che esiste già come parola non significativa.

Per creare un sinonimo:

1. Nella scheda Amministrazione, accedere a Conoscenza, Cerca, Motore di ricerca SC, Sinonimi.

   Viene visualizzata la pagina Elenco Sinonimi.

2. Fare clic su Crea nuovo.

   Viene visualizzata la pagina Crea nuovi sinonimi.

3. Immettere la parola o frase che si desidera definire come sinonimo nel campo Sinonimi.

4. Fare clic su Salva.

   La pagina Crea sinonimi si chiude e viene visualizzata la pagina Synonyms Detail che consente di verificare la parola o frase aggiunta. Il nuovo sinonimo viene visualizzato nella pagina Elenco Sinonimi.

Visualizzazione di sinonimi

È possibile visualizzare le informazioni di riepilogo per ciascun sinonimo.

Per visualizzare i sinonimi, selezionare la scheda Amministrazione e successivamente Conoscenza, Cerca, Motore di ricerca SC, Sinonimi.

Viene visualizza la pagina Elenco Sinonimi in cui è possibile modificare le parole chiave predefinite oppure definire parole chiave personalizzate tramite i seguenti campi:

Parola chiave

Consente di definire una parola chiave da ricercare. Questo campo viene visualizzato soltanto quando si fa clic su Mostra filtro.

Sinonimo

Consente di definire un sinonimo da ricercare. Questo campo viene visualizzato soltanto quando si fa clic su Mostra filtro.

Altri argomenti di ricerca

Consente di definire criteri di ricerca aggiuntivi. Questo campo viene visualizzato soltanto quando si fa clic sul collegamento Altro nel riquadro Ricerca conoscenza.

Elenco sinonimi

Consente di visualizzare le coppie di parole chiave e sinonimi definite nel prodotto. Per ciascuna parola chiave visualizzata nella colonna Parola chiave, nella colonna Sinonimo vengono visualizzati uno o più sinonimi.

Nella pagina Elenco Sinonimi è possibile svolgere le seguenti attività:

- Creare un sinonimo. (a pagina 1028)
- Modificare un sinonimo. (a pagina 1029)

Modifica di un sinonimo

È possibile modificare un sinonimo.

Per modificare un sinonimo:

1. Fare clic con il pulsante destro del mouse sul termine desiderato nell'elenco e selezionare Modifica dal menu di scelta rapida.

   Viene visualizzata la pagina Aggiorna sinonimo.

2. Immettere la parola o frase che si desidera definire come termine speciale nel campo Sinonimo.
3. Fare clic su Salva.

   La pagina Aggiorna sinonimo si chiude e viene visualizzata la pagina Dettagli sinonimo che consente di verificare la parola o frase aggiunta. Il termine aggiornato viene visualizzato nella pagina Elenco Sinonimi.

Impostazioni di analisi

Quando si pubblica un documento nell'archivio della conoscenza, viene effettuata l'analisi delle informazioni immesse nei campi Titolo, Riepilogo, Problema e Risoluzione del documento per estrapolare parole chiave. Quando un utente effettua la ricerca nell'archivio della conoscenza, il prodotto confronta le parole chiave dalla query dell'utente con le parole chiave analizzate dall'archivio della conoscenza per produrre un elenco di risultati. La pagina Impostazioni di analisi consente di definire le impostazioni utilizzate per analizzare i documenti dell'archivio della conoscenza.

Nota: la funzionalità Impostazioni di analisi è disponibile solo per il motore di ricerca SC predefinito.

Definizione di impostazioni di analisi

Quando si pubblica un documento nell'archivio della conoscenza, viene effettuata l'analisi delle informazioni immesse nei campi Titolo, Riepilogo, Problema e Risoluzione del documento per estrapolare parole chiave. Quando un utente effettua la ricerca nell'archivio della conoscenza, il prodotto confronta le parole chiave dalla query dell'utente con le parole chiave analizzate dall'archivio della conoscenza per produrre un elenco di risultati.

Per definire le impostazioni da usare per l'analisi dei documenti nell'archivio della conoscenza, aprire la scheda Amministrazione selezionando Conoscenza, Cerca, Impostazioni di analisi.

Viene visualizzata la pagina Impostazioni di analisi ed è possibile utilizzare i seguenti campi per definire le impostazioni:

Numero massimo di parole chiave per ricerca

Consente di definire il numero massimo di parole chiave da estrarre quando il prodotto effettua l'analisi del testo di ricerca.

Impostazione predefinita: 20

Nota: l'intervallo valido è 1-100. Tuttavia, l'amministratore della conoscenza CA SDM può modificare il valore all'interno di questo intervallo in base alle esigenze e ai parametri di ricerca di un determinato archivio della conoscenza. Per aumentare la velocità, utilizzare un numero inferiore di parole chiave per la ricerca.

Lingua

Consente di specificare il tipo di lingua da utilizzare per eseguire l'analisi. Selezionare una delle impostazioni riportate di seguito:

Inglese

Consente di eseguire alcuni tipi di elaborazione specifici della lingua inglese (ad esempio l'eliminazione dei plurali) durante una ricerca, ove possibile.

Altre lingue europee

Consente di eseguire la ricerca solo nelle lingue europee.

Coreano

Consente di eseguire la ricerca solo in coreano.

Estremo Oriente

Consente di eseguire la ricerca solo in altre lingue dell'Estremo Oriente.

Nota: negli ambienti operativi cinesi, giapponesi o coreani, verificare di aver compreso gli approcci di analisi disponibili e le limitazioni delle lingue che utilizzano set di caratteri multi-byte (MBCS) (a pagina 1032), prima di implementare Gestione della conoscenza sul proprio sistema per evitare di deludere le aspettative dell'utente.

Intervallo caratteri validi

Consente di definire l'intervallo di caratteri alfanumerici validi per effettuare l'analisi dei campi Titolo, Riepilogo, Problema e Risoluzione disponibili in un documento. Il prodotto considera gli altri caratteri come separatori.

Nota: se si seleziona Sì nell'elenco Riconosci termini speciali, il prodotto non analizza le parole e le frasi definite come termini speciali.

Impostazione predefinita: a-z, il quale indica che i caratteri alfabetici da a fino a z rappresentano caratteri validi per l'analisi.

Il campo Intervallo caratteri validi contiene le lettere appropriate utilizzate dall'analisi. Le lettere non presenti nel campo Intervallo caratteri validi verranno rimosse.

I valori consigliati per le diverse lingue sono i seguenti:

Lingua	Intervallo caratteri validi
Tedesco	a-zäöüß
Spagnolo	a-záéíóúüñ
Francese	a-zàäâçéèêëîïôùû
Portoghese brasiliano	a-zàáãçéêíóúü
Italiano	a-zàèéìîïù
Cinese semplificato	a-z
Giapponese	a-z
Cinese tradizionale	a-z
Coreano	a-z

Nota: il giapponese include l'intervallo “a-z” più un elenco di caratteri Katakana validi, con esclusione dei segni di interpunzione.

Rimuovi parole simili

Consente di specificare se il prodotto deve rimuovere le parole chiave simili per struttura dai gruppi utilizzati per la ricerca. È possibile scegliere una delle impostazioni seguenti:

Sì

Consente di rimuovere le parole chiave simili per struttura dai criteri di ricerca.

Nota: se si seleziona Sì, il prodotto rimuove anche le parole simili durante il salvataggio o la pubblicazione del documento. Se si seleziona Sì nella casella Rimuovi parole simili, si determina se è possibile effettuare una ricerca all'interno di un documento. Le parole simili potrebbero non essere state indicizzate e utilizzate in una ricerca successiva o nel recupero del documento.

No

Consente di mantenere le parole chiave simili per struttura come criteri di ricerca.

Impostazione predefinita: No

Rimuovi parole non significative

Consente di specificare se il prodotto deve rimuovere le parole non significative quando si analizzano i campi Titolo, Riepilogo, Problema e Risoluzione di un documento. È possibile scegliere una delle impostazioni seguenti:

Sì

Consente di rimuovere le parole non significative dai criteri di ricerca.

No

Consente di mantenere le parole non significative come criteri di ricerca.

Impostazione predefinita: Sì

Riconosci termini speciali

Consente di specificare se il prodotto deve considerare i termini speciali come entità singole o come parole multiple quando si analizzano i campi Titolo, Riepilogo, Problema e Risoluzione di un documento. È possibile scegliere una delle impostazioni seguenti:

Sì

Consente di elaborare i termini speciali come entità singole nei criteri di ricerca.

No

Consente di elaborare le parole che contengono termini speciali come entità separate nei criteri di ricerca.

Impostazione predefinita: Sì

Limitazioni di ricerca con i set di caratteri multi-byte

Assicurarsi di aver compreso i diversi metodi di analisi e le limitazioni delle lingue con set di caratteri multi-byte (MBCS) prima di implementare il sistema Gestione della conoscenza al fine di soddisfare le richieste degli utenti. Questa limitazione del prodotto influisce sulle funzionalità di ricerca effettuate su testo in giapponese, cinese o coreano nel sistema. Il meccanismo di analisi delle parole utilizzato dal meccanismo di ricerca può essere controllato nella pagina Impostazioni di analisi (a pagina 1029).

Per le impostazioni Inglese, Alle altre lingue europee e Coreano, il prodotto interpretano punti e spazi bianchi come elementi separatori delle parole. In tal modo, è possibile dividere il testo del documento in parole specifiche, ignorare le parole prive di significato e applicare sinonimi noti e termini speciali ai termini da ricercare.

Se si selezionano le impostazioni relative alle lingue dell'Estremo Oriente, la routine di analisi utilizza un approccio di analisi di tipo parola per parola perché tiene conto del fatto che alcune lingue dell'Estremo Oriente non utilizzano spazi per la delimitazione delle parole. Questa impostazione indica al programma di analisi di considerare ciascun carattere come una parola intera. L'impostazione si applica a tutto il testo ricercato. Poiché l'impostazione della lingua modifica il comportamento dell'analisi delle ricerche, è necessario ricreare tutto l'indice di ricerca se si seleziona o deseleziona l'impostazione lingua Estremo Oriente.

Documenti consigliati

Gli utenti CA SDM possono specificare i criteri relativi ad un elemento di interesse e il motore di ricerca individuerà i documenti della conoscenza corrispondenti, visualizzandoli nella pagina dei risultati di ricerca sotto forma di set di collegamenti ai "documenti consigliati". La query di ricerca può essere definita anche come parola chiave o set di parole (o frase) che identificano il concetto desiderato che potrebbe essere contenuto in uno o più documenti.

L'elenco dei documenti che soddisfano i criteri di ricerca viene ordinato e classificato (dal più alto al più basso) in modo che i documenti più rilevanti vengano presentati per primi nei risultati della ricerca. L'uso dei documenti consigliati permette agli utenti di impiegare meno tempo nella ricerca delle informazioni desiderate.

Per fornire un set di documenti corrispondenti, ordinati in maniera rapida secondo determinati criteri, il motore di ricerca raccoglie i dati secondo il tipo di condizione (frase, parole chiave o categoria) configurato dall'amministratore nella pagina Crea documenti consigliati.

Ulteriori informazioni:

Creazione di documenti consigliati (a pagina 1033)
Modifica di una condizione di un documento consigliato (a pagina 1035)
Visualizzazione di documenti consigliati (a pagina 1035)
Ricerca di documenti consigliati (a pagina 1036)

Creazione di documenti consigliati

Gli amministratori possono creare documenti consigliati in modo che possano essere trovati dagli utenti quando specificano criteri per un elemento desiderato.

Nota: in caso di installazione dell'opzione multi-tenancy, selezionare il titolare appropriato dall'elenco a discesa. L'opzione pubblica (condivisa) consente di creare l'oggetto per tutti i titolari.

Per creare un documento consigliato:

1. Nella scheda Amministrazione accedere a Conoscenza, Cerca, Documenti consigliati.

   Viene visualizzato l'elenco dei documenti consigliati.

2. Fare clic su Crea nuovo.

   Viene visualizzata la pagina Crea nuovi documenti consigliati.

3. Completare i campi seguenti in modo appropriato.

   Documento della conoscenza

   Consente di specificare un documento della conoscenza. In alternativa, è possibile fare clic sull'icona Cerca per aprire la pagina per la ricerca del documento della conoscenza.

   Tipo di condizione

   Consente di specificare un tipo di condizione (a pagina 1034) che deve essere usato dal motore di ricerca per ordinare e ricercare le corrispondenze del documento.

   - Se si imposta Corrispondenza esatta, Frase esatta o Parole chiave come tipo di condizione, viene visualizzato un campo di testo. È possibile immettere una frase o parola chiave che identifichi il concetto che deve contenere il documento.
   - Se si imposta Categoria della conoscenza come tipo di condizione, viene visualizzato il collegamento Categoria della conoscenza. È possibile specificare una categoria della conoscenza da associare al documento.

   Stato

   Indica se lo stato del record è attivo o inattivo.

   Fare clic su Salva.

   Il nuovo documento consigliato viene salvato nell'archivio della conoscenza e viene visualizzato nella pagina Elenco Documenti consigliati.

Campo Tipo di condizione

Il motore di ricerca ricerca i documenti utilizzando i seguenti tipi di condizioni:

Corrispondenza esatta

Ricerca i documenti utilizzando la frase di ricerca immessa nel campo del testo da ricercare. Viene rilevata una corrispondenza solo se il motore di ricerca trova esattamente tutte le stesse parole contenute nella frase.

Frase esatta

Ricerca i documenti utilizzando esattamente la frase di ricerca immessa nel campo del testo da ricercare. Viene rilevata una corrispondenza solo se il motore di ricerca trova il set o la sequenza esatti in una frase.

Parole chiave

Ricerca i documenti utilizzando le parole chiave immesse nel campo del testo da ricercare. Viene rilevata una corrispondenza solo se il motore di ricerca trova tutte le parole chiave.

Categoria della conoscenza

Ricerca i documenti utilizzando la categoria della conoscenza. Viene rilevata una corrispondenza solo se l'utente seleziona una categoria configurata per i documenti consigliati.

Modifica di una condizione di un documento consigliato

È possibile aggiornare la condizione di un documento consigliato.

Per modificare una condizione di un documento consigliato:

1. Nella scheda Amministrazione accedere a Conoscenza, Cerca, Documenti consigliati.

   Viene visualizzata la pagina Elenco documenti consigliati.

2. Per modificare una condizione, fare clic con il pulsante destro del mouse sul titolo nella colonna Condizione.

   Viene visualizzata la pagina Aggiorna documento.

3. Compilare i campi in modo appropriato.
4. Fare clic su Salva.

   La condizione aggiornata viene visualizzata su Elenco documenti consigliati.

Visualizzazione di documenti consigliati

È possibile visualizzare le informazioni di riepilogo per ciascun documento consigliato.

Per visualizzare i documenti consigliati, selezionare Cerca e successivamente Documenti consigliati nella scheda Amministrazione.

Viene visualizzata la pagina dell'elenco dei documenti consigliati che mostra le seguenti colonne:

Condizione

Indica la condizione usata dal motore di ricerca per ordinare il documento e trovare le corrispondenze.

Documento della conoscenza

Visualizza i documento nel set dei risultati.

Autore

Specifica l'autore del documento della conoscenza.

Data modifica

Visualizza la data dell'ultima modifica apportata al documento.

Dalla pagina Elenco documenti consigliati, è possibile svolgere le seguenti attività:

- Creare un documento consigliato. (a pagina 1033)
- Modificare una condizione di un documento consigliato. (a pagina 1035)
- Ricercare documenti consigliati. (a pagina 1036)

Ricerca di documenti consigliati

È possibile utilizzare la funzione di ricerca per filtrare l'elenco dei documenti consigliati e visualizzare esclusivamente gli elementi che si desidera vedere.

Nota: in caso di installazione dell'opzione multi-tenancy, la pagina di elenco visualizzerà le impostazioni Titolare e Dati pubblici nel filtro di ricerca. L'opzione Dati pubblici può essere inclusa o esclusa per i dati del titolare: la ricerca viene eseguita unicamente per gli oggetti pubblici. Nelle pagine dei dettagli, selezionare il titolare appropriato dall'elenco. Se si seleziona <vuoto>, l'oggetto è pubblico.

Per cercare un documento consigliato:

1. Nella scheda Amministrazione, accedere a Conoscenza, Cerca, Risultati consigliati.

   Viene visualizzato l'elenco dei documenti consigliati.

2. Fare clic su Mostra filtro.
3. Compilare i campi in modo appropriato. Per i campi seguenti sono necessarie ulteriori spiegazioni.

   Tipo

   Indica il tipo di condizione usato per trovare le corrispondenza e visualizzare il collegamento del documento consigliato

   Phrase/Keywords

   Indica le informazioni della query di ricerca usate per identificare il concetto desiderato nel contenuto del documento.

   Fare clic su Cerca.

   L'elenco dei documenti consigliati viene compilato con tutti gli elementi che corrispondono ai criteri di ricerca.

Impostazione delle impostazioni di ricerca predefinite

È possibile impostare opzioni di ricerca predefinite che vengano visualizzate quando gli utenti ricercano la conoscenza tramite il campo di ricerca.

Nota: queste opzioni di ricerca vengono sovrascritte da qualsiasi eventuale impostazione di ricerca personalizzata definita dagli utenti nella finestra Preferenze o da eventuali opzioni di ricerca aggiuntive nel riquadro Ricerca della conoscenza della scheda Conoscenza o nel riquadro Categorie della conoscenza della scheda Amministrazione.

Per definire le impostazioni di ricerca predefinite

1. Dalla scheda Amministrazione, accedere a Conoscenza, Cerca, Impostazioni di ricerca.

   Viene visualizzata la pagina Opzioni di ricerca.

2. Selezionare le seguenti opzioni secondo necessità:

   Risultati consigliati

   Consente di specificare il numero di documenti da visualizzare nell'elenco dei risultati della ricerca.

   Campi ricerca predefiniti

   Consente di specificare i campi predefiniti da includere nelle ricerche per parole chiave. Selezionare una casella di controllo per includere il campo corrispondente nelle ricerche predefinite. Deselezionare una casella di controllo per escludere il campo corrispondente dalle ricerche predefinite. È possibile utilizzare i seguenti campi del documento per le ricerche:

   - Titolo
   - Riepilogo
   - Problema
   - Risoluzione
   - Allegati

   Impostazioni di ricerca per tutte le fonti

   Consente di specificare se le ricerche possono includere tutte le fonti della conoscenza. Ad esempio, categorie della conoscenza e aree Richiesta.

Impostazioni di ricerca in contesto Ticket

Consente di specificare se le ricerche possono contenere tutti i campi definiti in un ticket di Service Desk (Incidente, Problema, Issue, Ordine di cambiamento o Richiesta).

- Per queste opzioni, selezionare *uno* dei seguenti tipi di corrispondenza:

- **Almeno una delle parole (OR)** - Consente di inserire nel set dei risultati un documento contenente una delle parole disponibili nella casella Cerca. Questa opzione è quella predefinita.
- **Tutte le parole (AND)** - Consente di inserire nel set dei risultati un documento solo se contiene tutte le parole disponibili nella casella Cerca.

Fare clic su Salva.

Le impostazioni di ricerca predefinite vengono configurate.

Opzioni integrazione CA SDM

Per l'integrazione CA SDM, è possibile usare le seguenti opzioni di configurazione:

Corrispondenza campi

Consente di specificare quali campi CA SDM compilare con le informazioni Gestione della conoscenza e se le informazioni esistenti devono essere sovrascritte o meno.

Configurazione ricerca problematiche

Consente di selezionare i campi in cui effettuare la ricerca quando si preme il pulsante Cerca in conoscenza.

Configurazione della ricerca di Issue

Seleziona i campi della ricerca quando si fa clic sul pulsante Cerca in un ticket.

Configurazione della ricerca di Richieste/Incidenti/Problemi

Seleziona i campi della ricerca quando si fa clic sul pulsante Cerca in un ticket.

Suggerisci conoscenza

Consente di selezionare i campi in cui effettuare la ricerca quando si preme il pulsante per la visualizzazione della conoscenza prima del salvataggio in un ticket.

Ulteriori informazioni:

Definizione del Mapping campi (a pagina 1039)
Definizione della configurazione della ricerca questione (a pagina 1041)
Definizione delle configurazione della ricerca di richiesta/incidente/problema (a pagina 1042)
Consigli della conoscenza (a pagina 1043)
Definizione delle categorie questione (a pagina 1044)
Definizione di aree richiesta/incidente/problema (a pagina 1045)
Configurazione di policy self-service (a pagina 1046)

Definizione del Mapping campi

Gli amministratori possono usare il riquadro Mapping campi per specificare quali campi devono essere completati con le informazioni Gestione della conoscenza e se le informazioni esistenti devono essere sovrascritte o meno.

Per definire i campi in Service Desk per Gestione della conoscenza:

1. Nella scheda Amministrazione, selezionare Conoscenza, Integrazione Service Desk, Mapping campi.

   Viene visualizzata la pagina Mapping campi.

2. Completare i campi seguenti in modo appropriato:

   Inserisci valori Service Desk da Gestione della conoscenza

   Consente di specificare se utilizzare le informazioni di Gestione della conoscenza per completare i campi relativi alle questioni o alle richieste di Service Desk.

   - Selezionare la casella di controllo per visualizzare i campi nelle colonne Gestione della conoscenza, Inserisci valori Service Desk non specificati e Sovrascrivi valori Service Desk e specificare le informazioni Gestione della conoscenza da inserire nei campi relativi alle questioni o alle richieste Service Desk.
   - Deselezionare la casella di controllo per disattivare i campi nelle colonne Gestione della conoscenza, Inserisci valori Service Desk non specificati e Sovrascrivi valori Service Desk. In tal caso, gli utenti devono inserire manualmente le questioni o le richieste di Service Desk create in Gestione della conoscenza.

   Impostazione predefinita: questa casella di controllo è selezionata.

Service Desk

Identifica i campi in problemi o richieste che corrispondono a campi elencati nella colonna Gestione della conoscenza.

Per ciascuna una casella di controllo selezionata nella colonna Inserisci valori Service Desk non specificati, nella questione o nella richiesta vengono visualizzate le informazioni del campo corrispondente nella colonna Gestione della conoscenza.

Gestione della conoscenza

Identifica i campi Gestione della conoscenza che corrispondono ai campi Service Desk elencati nella colonna Service Desk.

Per ciascuna una casella di controllo selezionata nella colonna Inserisci valori Service Desk non specificati, nella questione o nella richiesta vengono visualizzate le informazioni del campo corrispondente nella colonna Gestione della conoscenza.

Nella colonna Gestione della conoscenza sono disponibili due elenchi a discesa:

- Il primo elenco a discesa corrisponde al campo Riepilogo nella colonna Service Desk e riporta i valori del campo Gestione della conoscenza (Titolo, Riepilogo o Problema) che vengono inseriti nel campo Riepilogo in una questione o richiesta.

Impostazione predefinita: Riepilogo.

- Il secondo elenco a discesa corrisponde al campo Descrizione nella colonna Service Desk e riporta i valori del campo Gestione della conoscenza (Titolo, Riepilogo o Problema) che vengono inseriti nel campo Descrizione in una questione o richiesta.
- **Impostazione predefinita**: Problema.

Inserisci valori Service Desk non specificati

Consente di specificare quali campi vuoti di una questione o richiesta Service Desk devono essere compilati con le informazioni fornite da Gestione della conoscenza.

- Selezionare una casella di controllo per associare le informazioni del campo Gestione della conoscenza con il campo corrispondente, nel caso in cui sia vuoto.
- Deselezionare la casella di controllo se non si desidera associare le informazioni del campo Gestione della conoscenza al campo Service Desk corrispondente.

Impostazione predefinita: le caselle di controllo che corrispondono

ai campi Riepilogo, Descrizione, Prodotto, Asset e Area Richiesta sono sempre selezionate in Service Desk.

Sovrascrivi valori Service Desk

Consente di specificare di una questione o richiesta Service Desk devono essere sovrascritti con le informazioni fornite da Gestione della conoscenza.

- Selezionare una casella di controllo per sostituire le informazioni del campo Service Desk con quelle del campo Gestione della conoscenza corrispondente.
- Deselezionare la casella di controllo se non si desidera sostituire le informazioni del campo Service Desk con quelle del campo Gestione della conoscenza.

Queste caselle di controllo sono disponibili solo quando si selezionano le caselle di controllo corrispondenti nella colonna Inserisci valori Service Desk non specificati.

Impostazione predefinita: tutte le caselle di controllo di sovrascrittura dei valori Service Desk vengono deselezionate.

Fare clic su Salva.

Viene definito il mapping campi.

Definizione della configurazione della ricerca questione

È possibile specificare i campi di una questione in cui deve essere eseguita la ricerca quando si seleziona il pulsante Cerca in conoscenza su un ticket. I campi selezionati vengono copiati nei campi corrispondenti di Filtro di ricerca nella scheda Conoscenza della finestra Dettagli Questione. I campi Filtro di ricerca del ticket vengono compilati quando si seleziona la scheda Conoscenza o il pulsante Ripristina filtro nella scheda Conoscenza.

Per definire i campi in una questione da utilizzare per le ricerche nell'archivio della conoscenza:

1. Nella scheda Amministrazione, selezionare Conoscenza, Integrazione CA SDM, Configurazione di ricerca Questioni.

   Viene visualizzata la pagina Integrazione CA SDM.

2. Selezionare i campi che si desidera siano disponibili per ricerche nell'Archivio della conoscenza.

   - Riepilogo
   - Descrizione
   - Elemento della configurazione
   - Priorità
   - Categoria
   - Causa principale
   - Prodotto

   Nota: non è possibile selezionare sia il campo Riepilogo che il campo Descrizione.

3. Selezionare l'opzione "Avvia automaticamente la ricerca quando la scheda Conoscenza di una Richiesta è stata selezionata" per effettuare automaticamente le ricerche nell'archivio della conoscenza quando viene selezionata la scheda Conoscenza nella pagina Dettagli.

4. Fare clic su Salva.

   La ricerca Questione viene configurata.

Definizione delle configurazione della ricerca di richiesta/incidente/problema

È possibile specificare in quali campi di una richiesta, incidente o problema deve essere effettuata la ricerca quando si seleziona il pulsante Cerca in conoscenza su un ticket. I campi selezionati vengono copiati nei campi corrispondenti di Filtro di ricerca nella scheda Conoscenza della finestra Dettagli Ticket. I campi Filtro di ricerca del ticket vengono compilati quando si seleziona la scheda Conoscenza o il pulsante Ripristina filtro nella scheda Conoscenza.

Per definire i campi in una richiesta, incidente o problema da utilizzare per le ricerche dell'archivio della conoscenza:

1. Nella scheda Amministrazione, selezionare Conoscenza, Integrazione CA SDM, Configuraz ricerca Richieste/Incidenti/Problemi.

   Viene visualizzata la pagina Integrazione CA SDM.

2. Selezionare i campi che si desidera siano disponibili per ricerche nell'Archivio della conoscenza.

   - Riepilogo
   - Descrizione
   - Elemento della configurazione
   - Gravità
   - Impatto
   - Urgenza
   - Priorità
   - Area richiesta
   - Causa principale

   Nota: non è possibile selezionare sia il campo Riepilogo che il campo Descrizione.

3. Selezionare l'opzione "Avvia automaticamente la ricerca quando la scheda Conoscenza di una Richiesta è stata selezionata" per effettuare automaticamente le ricerche nell'archivio della conoscenza quando viene selezionata la scheda Conoscenza nella pagina Dettagli.

4. Fare clic su Salva.

   I campi in una richiesta, incidente o problema da utilizzare per le ricerche dell'archivio della conoscenza vengono configurati.

Consigli della conoscenza

Quando creano un nuovo ticket nell'interfaccia self-service, i dipendenti ed i clienti possono, laddove permesso, visualizzare un elenco di consigli della conoscenza.

Se viene trovata una soluzione ma il ticket non viene salvato, è possibile far considerare i documenti suggeriti tramite il sistema di classificazione self-service nel modulo documento. Questo sistema di classificazione varia a seconda delle impostazioni delle policy self-service definite nella pagina Impostazioni di ricerca.

I dati recuperati possono essere usati per i report, i dashboard e per le ricerche nell'archivio della conoscenza, dove gli utenti possono filtrare i documenti il cui ticket è stato risolto con successo.

I vantaggi della funzionalità self-service derivano dalla possibilità di ridurre il numero di chiamate di assistenza e di ticket ridondanti creati, e conseguentemente anche le spese operative.

L'amministratore deve abilitare questa funzionalità prima dell'uso e configurare categorie questioni e aree richiesta appropriate per le quali deve essere suggerita la conoscenza nell'interfaccia self-service.

Definizione delle categorie questione

È possibile definire categorie questione per le quali viene suggerita la conoscenza ai clienti e dipendenti al momento della creazione del ticket.

È anche possibile contrassegnare la caratteristica Suggerisci conoscenza come attiva o inattiva. Quando viene contrassegnata questa caratteristica come inattiva, non risulterà più disponibile a clienti e dipendenti, ma rimarrà disponibile nel database per uso futuro. Se si decide di utilizzare questa caratteristica in futuro, è possibile tornare al passaggio precedente e contrassegnarla come attiva.

Per definire categorie questione per il suggerimento della conoscenza:

1. Nella scheda Amministrazione, selezionare Conoscenza, Integrazione Service Desk, Suggerisci conoscenza, Categorie Questione.

   Viene visualizzata la pagina Suggerisci conoscenza per categorie Questione.

2. Selezionare l'opzione **Non suggerire conoscenza** per contrassegnare la caratteristica Suggerisci conoscenza come attiva.

   Predefinito: Non attivo

   Se si seleziona questa funzionalità, vengono visualizzate le seguenti opzioni:

   Per impostazione predefinita, la conoscenza sarà:

   Consigliato

   Indica che si *desidera* che la conoscenza venga suggerita per tutte le categorie questione, eccetto che per le definizioni nell'elenco categorie questione.

   Non consigliato

   Indica che si *non* si desidera che la conoscenza venga suggerita per tutte le categorie questione, eccetto che per le definizioni nell'elenco categorie questione.

Per tutte le Categorie di Questione eccetto le seguenti:

Visualizza l'elenco delle aree di richiesta in cui la conoscenza viene consigliata o non consigliata a dipendenti e clienti nell'interfaccia self-service. All'utente self-service non è consentito modificare le aree della richiesta poiché sono di sola lettura.

3. Fare clic su *uno* dei seguenti pulsanti:

   Aggiungi

   Aggiunge all'elenco l'area di richiesta selezionata.

   Rimuovi

   Rimuove dall'elenco l'area di richiesta selezionata.

   Rimuovi tutto

   Rimuove dall'elenco tutte le aree di richiesta.

   Salva

   Salva le informazioni dell'area di richiesta nell'archivio della conoscenza.

   Vengono definite le categorie questione.

Definizione di aree richiesta/incidente/problema

È possibile definire aree richiesta, problema e incidente per le quali suggerisce la conoscenza ai clienti e dipendenti al momento della creazione del ticket.

È anche possibile contrassegnare la caratteristica Suggerisci conoscenza come attiva o inattiva. Quando viene contrassegnata questa caratteristica come inattiva, non risulterà più disponibile a clienti e dipendenti, ma rimarrà disponibile nel database per uso futuro. Se si decide di utilizzare questa caratteristica in futuro, è possibile tornare al passaggio precedente e contrassegnarla come attiva.

Per definire aree richiesta/incidente/problema per il suggerimento della conoscenza:

1. Nella scheda Amministrazione, selezionare Conoscenza, Integrazione CA SDM, Suggerisci conoscenza, Aree Richiesta/Incidente/Problema.

   Viene visualizzata la pagina Suggerisci conoscenza per aree Richiesta/Incidente/Problema.

2. Selezionare l'opzione **Non suggerire conoscenza** per contrassegnare la caratteristica Suggerisci conoscenza come attiva.

   Predefinito: Non attivo

   Se si seleziona questa funzionalità, vengono visualizzate alcune altre opzioni aggiuntive:

Per impostazione predefinita, la conoscenza sarà:

Consigliato

Selezionare questa opzione se si desidera che la conoscenza venga suggerita per tutte le aree richiesta/incidente/problema, eccetto quelle definite nell'elenco Area Richiesta.

Non consigliato

Selezionare questa opzione se *non* si desidera che la conoscenza venga suggerita per tutte le aree richiesta/incidente/problema, eccetto quelle definite nell'elenco Area Richiesta.

Per tutte le aree Richiesta/Incidente/Problema eccetto le seguenti:

Visualizza l'elenco delle aree di richiesta in cui la conoscenza viene consigliata o non consigliata a dipendenti e clienti nell'interfaccia self-service. All'utente self-service non è consentito modificare le aree della richiesta poiché sono di sola lettura.

Fare clic su Salva.

Vengono definite le aree Richiesta/Incidente/Problema per il suggerimento della conoscenza.

Configurazione di policy self-service

È possibile configurare policy self-service che registrino i documenti in base a un set di scenario utente.

Per configurare le policy self-service:

1. Nella scheda Amministrazione, selezionare Conoscenza, Integrazione CA SDM, Suggerisci conoscenza, Configurazione self-service.

   Viene visualizzata la pagina Impostazioni di ricerca.

2. Specificare le impostazioni delle policy appropriate per registrare i documenti e salvare i ticket evasi quando si verificano i seguenti scenari utente:

   - L'utente non ha aperto alcuno dei documenti suggeriti
   - L'utente ha aperto un documento suggerito
   - L'utente ha accettato il documento suggerito come soluzione al problema
   - L'utente ha ricercato la conoscenza, aperto il documento ed è uscito

   Fare clic su Salva.

   Le impostazioni delle policy self-service vengono salvate.

Indagine soluzione

Indagine soluzione consente di raccogliere e analizzare il feedback dei clienti sulle prestazioni sul documento della conoscenza. È possibile modificare le impostazioni dell'indagine selezionando Conoscenza e Indagine soluzione dall'interfaccia di amministrazione. L'indagine compare in un documento della conoscenza pubblicato e permette ai clienti, agli utenti guest e ai dipendenti di classificare l'efficacia del documento della conoscenza.

Questa funzionalità include i seguenti componenti:

- Impostazioni FAQ
- Impostazioni indagine

Ulteriori informazioni:

Definizione di impostazioni FAQ (a pagina 1047)
Definizione di impostazioni di indagine soluzione (a pagina 1049)

Definizione di impostazioni FAQ

La finestra Impostazioni FAQ consente di impostare i parametri con i quali il prodotto calcola la classificazione FAQ assegnata a ciascun documento. Il prodotto calcola la classificazione FAQ in base ai seguenti criteri:

- Frequenza di consultazione di un documento in passato
- Utilità del documento per gli utenti
- Diminuzione dell'efficacia del documento nel tempo

Per impostazione predefinita, i documenti vengono visualizzati nella pagina Elenco Documenti in base alla classificazione FAQ, ossia in base al grado di utilità. I documenti più utili vengono visualizzati in alto nell'elenco, ma tendono a scendere di graduatoria in quanto gli utenti apprendono le soluzioni ai problemi.

Per definire le impostazioni FAQ:

1. Selezionare Conoscenza, Indagine soluzione e Impostazioni FAQ nella scheda Amministrazione.

   Viene visualizzata la pagina Impostazioni FAQ.

2. Completare i campi seguenti in modo appropriato:

   Ultimo aggiornamento

   Consente di eseguire il Servizio Classificazione FAQ e di visualizzare la data dell'ultimo aggiornamento delle classificazioni FAQ.

   - Selezionare la casella di controllo Esegui servizio Classificazione FAQ per effettuare il calcolo FAQ mediante le impostazioni disponibili in questa finestra.
   - Selezionare la casella di controllo Esegui servizio Classificazione FAQ per terminare il calcolo FAQ.

   Pianifica

   Consente di definire la frequenza con cui il prodotto aggiorna le classificazioni FAQ. In questo campo sono disponibili i seguenti componenti:

   Esegui calcolo FAQ ogni...

   Consente di specificare l'intervallo di tempo che intercorre tra gli aggiornamenti della classificazione FAQ dei documenti.

   Impostazione predefinita: 1 giorno

   Da

   Consente di specificare l'ora del giorno in cui il prodotto dovrebbe avviare nuovamente il calcolo delle classificazioni FAQ.

   Impostazione predefinita: 00:00 (12:00 A.M.)

   A

   Consente di specificare la data del giorno in cui il prodotto dovrebbe interrompere il calcolo delle classificazioni FAQ indipendentemente che il calcolo sia terminato.

   Impostazione predefinita: 07:00 (7:00 A.M.)

   Nota: questa impostazione viene attivata il giorno successivo all'installazione del prodotto. Ad esempio, se si installa il prodotto il 19 aprile 2008, il server FAQ viene eseguito la prima volta il 20 aprile 2008.

Durata

Consente di specificare per quante volte viene ricalcolata la classificazione FAQ prima che raggiunga 0. In base al valore specificato, la classificazione FAQ del documento diminuisce fino a raggiungere 0 nel qual caso viene visualizzata in fondo all'elenco di documenti (quando si ordina l'elenco in base alla valutazione FAQ).

Impostazione predefinita: 180

Ad esempio, se il valore Durata è 180 per un documento con classificazione 4 (molto utile), la classificazione FAQ del documento diventerà 0 (zero) nel momento in cui il prodotto avrà calcolato la classificazione FAQ per 180 volte.

Nota: per impostazione predefinita, il calcolo per priorità FAQ richiede dati bu_trans per almeno 180 giorni, dove 180 rappresenta il fattore di durata. Se si modifica il fattore di durata FAQ con un valore superiore a 365 giorni, è necessario estendere anche le regole di archiviazione per la tabella bu_trans.

Giorni nuovo

Consente di specificare il numero di giorni in cui un documento creato o importato di recente viene visualizzato nella cartella Nuovi documenti della scheda Conoscenza.

Impostazione predefinita: 5 giorni

Classificazione

Consente di specificare la classificazione predefinita (Non utile, Abbastanza utile o Molto utile) per i documenti che gli utenti hanno visualizzato ma non classificato.

Impostazione predefinita: Abbastanza utile

Fare clic su Salva.

Le impostazioni FAQ sono definite.

Definizione di impostazioni di indagine soluzione

È possibile usare la pagina Impostazioni indagine per specificare come deve essere visualizzato il documento della conoscenza quando l'utente vi accede per risolvere un problema o rispondere a una domanda.

Per definizione le impostazioni di indagine soluzione:

1. Selezionare Conoscenza, Indagine soluzione e Impostazioni indagine nella scheda Amministrazione.

   Viene visualizzata la pagina Impostazioni indagine.

2. Completare i campi seguenti in modo appropriato. Fare clic su Salva.

   Vengono definite le impostazioni dell'indagine soluzione.

Impostazioni di sistema di Gestione della conoscenza

È possibile impostare le informazioni predefinite da visualizzare all'accesso nella scheda Conoscenza, il formato di visualizzazione delle categorie nel riquadro Categorie della conoscenza della scheda Amministrazione e il numero di documenti da includere nell'elenco Soluzioni principali nella pagina iniziale di Gestione della conoscenza.

Ulteriori informazioni:

Configurazione delle impostazioni generali (a pagina 1050)

Configurazione delle impostazioni generali

È possibile specificare quali informazioni predefinite vengono visualizzate nella scheda Conoscenza (all'accesso), il formato di visualizzazione delle categorie nel riquadro Categorie della conoscenza della scheda Amministrazione e il numero di documenti da includere nell'elenco Soluzioni principali nella pagina principale Gestione della conoscenza.

Procedere come descritto di seguito:

1. Selezionare Conoscenza, Sistema, Impostazioni generali nella scheda Amministrazione.

   Viene visualizzata la pagina Impostazioni generali.

2. Completare i campi seguenti in modo appropriato:

   Schermata iniziale strumento di ricerca

   Specifica le impostazioni predefinite visualizzate nella scheda Conoscenza. È possibile selezionare una delle tre opzioni indicate.

   - Apri con FAQ/Cerca—Visualizza i riquadri Categoria, Ricerca della conoscenza ed Elenco Documenti della conoscenza.
   - Apri con ID documento struttura della conoscenza—Visualizza la struttura della conoscenza con l'ID documento specificato nel campo corrispondente. È possibile tornare al documento della struttura conoscenza, quindi ai riquadri Categoria, Ricerca della conoscenza ed Elenco Documenti della conoscenza. **Impostazione predefinita:** Apri con FAQ/Cerca

Visualizzazione categoria

Consente di specificare il formato di visualizzazione delle categorie del documento nel riquadro Categorie della conoscenza nella scheda Amministrazione. È possibile selezionare una delle tre opzioni indicate.

- Mostra categorie in visualizzazione struttura—Presenta le categorie in una struttura gerarchica nel riquadro Categorie della conoscenza. È possibile espandere le categorie per visualizzare le sottocategorie associate. In questo modo, è possibile visualizzare contemporaneamente tutte le categorie della struttura.
- Mostra categorie in visualizzazione elenco—Presenta le categorie sotto forma di elenco nel riquadro Categorie della conoscenza. Quando si seleziona una categoria, le sottocategorie vengono visualizzate in un elenco. È possibile visualizzare contemporaneamente il livello corrente delle categorie o sottocategorie. Il collegamento Livello superiore consente di tornare al livello di categoria precedente.

Nota: se si dispone di oltre 250 categorie sotto la categoria superiore o sotto qualsiasi categoria, utilizzare l'opzione Mostra categorie in visualizzazione elenco e non la visualizzazione struttura.

Soluzioni principali

Specifica il numero di documenti da elencare nell'elenco Soluzioni principali nella pagina iniziale di CA SDM.

Impostazione predefinita: 10

Percorso file di indice EBR

Definisce la posizione per l'archiviazione dei file di indice EBR. CA SDM crea i file di indice EBR quando si salva e si pubblica un documento della conoscenza. A seconda del tipo di configurazione, considerare i punti seguenti durante la definizione del percorso per il file di indice EBR:

- Convenzionale: in caso di aggiornamento di CA SDM Versione 12.9 da r11.2 o da r12.X, è possibile scegliere di non utilizzare il percorso condiviso UNC. Se non è stato creato un percorso UNC, CA SDM utilizza il percorso predefinito per archiviare i file di indice EBR. Se si utilizza un'unità condivisa UNC, copiare manualmente le cartelle ebr/ebr_ADM dalla posizione predefinita ($NX_ROOT/site/) al percorso condiviso UNC.
- Disponibilità avanzata: in caso di aggiornamento alla configurazione con disponibilità avanzata da CA SDM r11.2 o r12.X, è necessario creare il percorso condiviso UNC e utilizzarlo per archiviare i file di indice EBR. Le credenziali UNC non sono obbligatorie per il percorso predefinito. Dopo aver creato il percorso UNC, copiare manualmente le cartelle ebr/ebr_ADM dalla posizione predefinita ($NX_ROOT/site/) al percorso condiviso UNC.

Importante. Il percorso dei file di indice EBR e il percorso dei file KEIT devono fare riferimento alle stesse credenziali UNC. A tale scopo, il percorso deve risiedere sullo stesso server.

Impostazione predefinita: $NX_ROOT/site/ebr

Percorso file di esportazione/importazione della conoscenza

Definisce la posizione per l'archiviazione dei pacchetti di esportazione/importazione KEIT durante un'operazione di esportazione/importazione. A seconda del tipo di configurazione, considerare i punti seguenti durante la definizione del percorso per il file KEIT:

- Convenzionale: in caso di aggiornamento a CA SDM Versione 12.9 da r11.2 o r12.X, è possibile scegliere di non utilizzare il percorso condiviso UNC. Se non è stato creato un percorso UNC, CA SDM utilizza il percorso predefinito per archiviare i file KEIT. Se si utilizza un'unità condivisa UNC, copiare manualmente le cartelle del pacchetto di esportazione/importazione dalla posizione predefinita ($NX_ROOT/site/keit) al percorso condiviso UNC.
- Disponibilità avanzata: in caso di aggiornamento alla configurazione con disponibilità avanzata da CA SDM r11.2 o r12.X, è necessario creare il percorso condiviso UNC e utilizzarlo per archiviare i file KEIT. Le credenziali UNC non sono obbligatorie per il percorso predefinito. Dopo aver creato il percorso UNC, copiare manualmente le cartelle del pacchetto di esportazione/importazione dalla posizione predefinita ($NX_ROOT/site/keit) al percorso condiviso UNC.

Importante. Il percorso dei file di indice EBR e il percorso dei file KEIT devono fare riferimento alle stesse credenziali UNC. A tale scopo, il percorso deve risiedere sullo stesso server.

Impostazione predefinita: $NX_ROOT/site/keit

Credenziali UNC

È possibile utilizzare questa opzione per creare credenziali UNC di accesso all'unità condivisa di rete per poter accedere ai file di indice EBR e ai pacchetti di esportazione/importazione. Utilizzare il collegamento Credenziali UNC per creare le credenziali UNC.

Nota: I percorsi UNC e le credenziali UNC sono obbligatori in caso di configurazione con disponibilità avanzata. Riavviare il servizio di CA SDM quando si modificano i dettagli UNC (percorsi UNC o credenziali UNC).

Notifiche indicizzazione documento

Consente di impostare un utente come destinatario delle notifiche di posta elettronica relative allo stato oppure quando si verifica un errore nell'indicizzazione del documento. Per ricevere le notifiche di posta elettronica, l'utente deve disporre di un indirizzo di posta elettronica nella tabella ca_contacts. È possibile usare la pagina Notifica per impostare i metodi di notifica per il record di contatto dell'assegnatario.

Importante. È necessario impostare un Assegnatario per ricevere le notifiche di indicizzazione del documento nella sezione Notifiche di indicizzazione documento. È necessario definire un indirizzo di posta elettronica valido nella scheda Notifica di questo contatto per abilitare le notifiche di posta elettronica.

3. Fare clic su Salva.

   Le impostazioni generali vengono configurate.

Nota: Quando si esegue la migrazione da una versione precedente di CA SDM alla configurazione con disponibilità avanzata, copiare manualmente i pacchetti di esportazione/importazione nella posizione condivisa UNC, specificata nel campo Percorso file di esportazione/importazione della conoscenza. Per i file di indice EBR, è possibile spostare manualmente le cartelle EBR/ebr_ADM nella posizione condivisa UNC o eseguire il percorso del comando pdm_k_reindex.

Capitolo 24: Amministrazione di Support Automation

Questa sezione contiene i seguenti argomenti:

Automatizzazione del supporto nel proprio ambiente (a pagina 1055)
Amministrazione degli analisti Support Automation (a pagina 1058)
Amministrazione degli utenti Support Automation (a pagina 1073)
Amministrazione delle notifiche relative all'attività di Support Automation (a pagina 1080)
Adattamenti pagine Support Automation (a pagina 1081)
Proprietà di sistema Support Automation (a pagina 1083)
Amministrazione delle code Support Automation (a pagina 1084)
Gestione dei modelli di ticket (a pagina 1086)
Impostazioni di amministrazione (a pagina 1086)
Personalizzazione degli strumenti Support Automation (a pagina 1089)
Amministrazione del registro sessione (a pagina 1097)
Report Support Automation (a pagina 1098)
Risoluzione dei ticket mediante l'assistenza in tempo reale (a pagina 1098)

Automatizzazione del supporto nel proprio ambiente

È possibile implementare una strategia di supporto utilizzando più processi e strumenti. CA SDM fornisce gli strumenti necessari per amministrare l'assistenza in tempo reale, sviluppare attività automatiche e fornire tramite vari canali di supporto.

È possibile usare i processi associati per creare e mantenere un ambiente che:

- Riduca la durata media delle chiamate di supporto
- Riduca i costi complessivi dell'attività di supporto
- Incrementi la percentuale di risoluzione
- Migliori la soddisfazione degli utenti finali

Assistenza in tempo reale

Assistenza in tempo reale fornisce supporto all'utente finale tramite strumenti che migliorano l'interazione remota tra gli analisti e gli utenti remoti. È possibile usare risposte automatiche predefinite per comunicare con l'utente finale. L'utente raccoglie informazioni personalizzate sul computer di un utente finale e intraprendere quindi le azioni necessarie per fornire supporto.

È possibile fornire assistenza in tempo reale utilizzando le seguenti interfacce:

Interfaccia analista Support Automation

Permette agli analisti di interagire con gli utenti finali e di fornire supporto durante le sessioni di assistenza.

Client dell'utente finale

Permette all'utente finale di conversare con l'analista mentre gli sta fornendo supporto per il suo computer.

Connettività Support Automation

L'analista e l'utente finale non comunicano mai direttamente. Quindi, non è necessaria una connettività peer-to-peer diretta tra questi due utenti. Tutti i trasferimenti dati vengono effettuati tramite il server allo scopo di garantire le comunicazioni anche nel caso in cui i computer degli utenti finali siano protetti da firewall restrittivi.

Per connettere i computer degli utenti finali, è possibile usare le seguenti connessioni:

Socket

La connessione mediante socket rappresenta il miglior metodo di connessione. Le connessioni socket sono quelle più veloci, poiché presentano un minor traffico, una latenza minima e forniscono la migliore efficienza di connessione in assoluto.

HTTP (o HTTPS)

L'uso di una connessione HTTP offre maggiori vantaggi rispetto a una connessione diretta tramite socket, perché i firewall aziendali possono talvolta bloccare le connessioni dirette tramite socket. Le connessioni HTTP generano tuttavia più traffico rispetto a quelle dirette tramite socket. A causa del maggior traffico e del uso più intensivo delle risorse di elaborazione del server, il numero di sessioni simultanee supportate è molto minore se la maggior parte delle connessioni viene effettuata tramite HTTP.

Proxy

Il proxy socket è una modalità operativa che consente al server Support Automation di distribuire parte delle operazioni che utilizzano in modo intensivo la CPU. Le operazioni di crittografia/decrittazione possono infatti essere trasferite dal server principale a un componente server nella DMZ (o in un'altra zona simile) all'interno della topologia della rete logica.

In genere il primo tentativo di connessione viene effettuato utilizzando la connessione diretta tramite socket. Se non è possibile effettuare questo tipo di connessione, viene utilizzata quella HTTP. È tuttavia possibile specificare impostazioni personalizzate per la connessione sul computer client per modificare questa sequenza.

Nota: per informazioni dettagliate su come configurare le impostazioni per le comunicazioni, consultare la *Guida in linea*.

Client dell'utente finale

Il client dell'utente finale connette gli utenti finali agli analisti durante le sessioni di assistenza in tempo reale. Gli utenti avviano una sessione chat con gli analisti in WebChat. Tuttavia, nel caso in cui sia necessario usare gli strumenti dell'interfaccia Analista Support Automation, CA SDM avvia il client sul computer dell'utente finale. Una volta avviato il client, l'utente finale visualizza le istruzioni corrispondenti al browser Web in uso.

Carico del server

Nelle distribuzioni di grandi dimensioni, un carico elevato sul server può ridurre le prestazioni dell'applicazione. Per questo motivo, è opportuno trasferire parte dell'elaborazione a uno o più proxy server effettuando le seguenti operazioni:

- Trasferendo la cifratura e decifratura dei dati in entrata e uscita per tutti gli analisi o client (utilizzando una connessione diretta al socket o HTTP)
- Trasferendo l'elaborazione del traffico HTTP da e ai clienti che utilizzano HTTP per connettersi al proxy socket

Componente server DMZ

In alcuni ambienti di rete, permettere al socket di accedere direttamente ai server delle applicazioni su cui è in esecuzione l'applicazione server Support Automation, pone dei rischi per la sicurezza. In questi ambienti è possibile usare un proxy socket in DMZ per fornire un componente middleman tra gli utenti di Internet e i server delle applicazioni. L'uso di un proxy socket in questo scenario consente di ridurre le operazioni di elaborazione del server principale.

Modalità di funzionamento del proxy socket

Il proxy socket funziona in questo modo:

1. Il proxy socket rimane in ascolto delle connessioni in arrivo dagli analisti o utenti finali sulla porta esterna configurata.
2. Stabilisce quindi una connessione peer con il server principale utilizzando la porta interna configurata per ciascuna connessione. Queste due connessioni vengono rispettivamente denominate connessione dell'utente finale e connessione del server.

3. Le connessioni dell'utente finale sono crittografate e il proxy server crittografa/decrittografa tutti i dati in entrata o uscita sulla/dalla connessione dell'utente finale.

   Nota: le connessioni server non sono crittografate.

4. Per ciascun pacchetto dati in arrivo, viene verificata la struttura del protocollo e viene validato il valore checksum prima del trasferimento dei dati al server principale tramite la connessione server.
5. Il server principale gestisce l'elaborazione della crittografia/decrittografia.
6. Il proxy socket chiude la connessione peer corrispondente appena viene chiusa la connessione dell'utente finale o del server.

Amministrazione degli analisti Support Automation

Gli analisti Support Automation controllano e gestiscono più Richieste degli utenti finali nel corso di sessioni di assistenza in tempo reale nell'ambiente. Gli analisti utilizzano gli strumenti Support Automation per interagire con gli utenti finali e fornire loro assistenza in tempo reale.

Possono accedere all'interfaccia tramite un ticket CA SDM, come un Incidente o la scheda Support Automation. È possibile gestire i livelli di accesso per impostare le autorizzazioni per gli strumenti utilizzati dagli analisti. È possibile abilitare e disabilitare strumenti Support Automation per titolari specifici. Se uno strumento risulta disabilitato per il titolare, gli analisti non possono usarlo durante le sessioni di assistenza.

Importante. L'interfaccia Analista Support Automation può essere eseguita solo in Windows. Per ulteriori informazioni sull'elenco di sistemi operativi supportati, consultare le *Note di rilascio*.

Ulteriori informazioni:

Introduzione (a pagina 1059)
Configurazione dell'assistenza in tempo reale per gli analisti (a pagina 1060)
Avvio dell'Assistenza in tempo reale da parte degli analisti (a pagina 1069)
Come configurare Assistenza in tempo reale per gli analisti (a pagina 1070)
Procedure utilizzabili dagli utenti finali per accedere alle sessioni di assistenza (a pagina 1071)
Procedure usate dagli analisti per automatizzazione il supporto per gli utenti finali (a pagina 1072)
Procedure utilizzate dagli analisti per fornire assistenza in tempo reale (a pagina 1073)

Introduzione

Prodotto: CA SDM

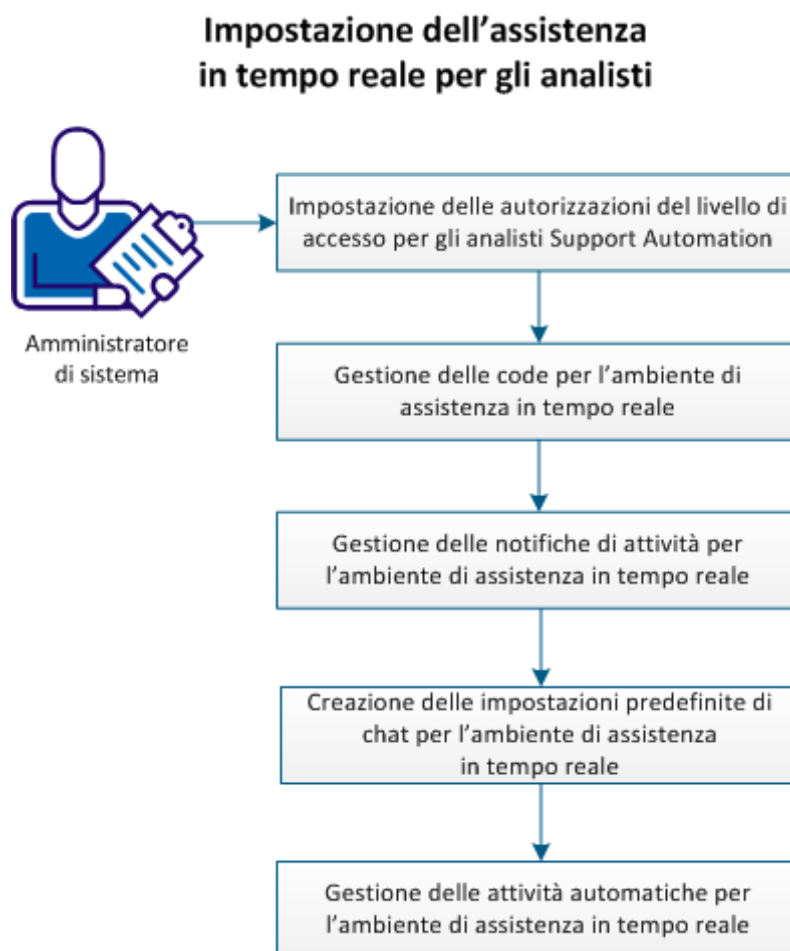
Versione: Versione 12.9

Sistema operativo: Windows e Linux

Questo scenario descrive la procedura seguita da un amministratore di sistema per configurare l'assistenza in tempo reale per gli analisti di Support Automation.

Configurazione dell'assistenza in tempo reale per gli analisti

In qualità di amministratori di sistema, è possibile configurare l'assistenza in tempo reale e gestire i livelli di accesso per impostare le autorizzazioni relative agli strumenti utilizzabili dagli analisti. È possibile abilitare e disabilitare strumenti Support Automation per titolari specifici. Se uno strumento risulta disabilitato per il titolare, gli analisti non possono usarlo durante le sessioni di assistenza.

Il diagramma seguente descrive la procedura per configurare l'assistenza in tempo reale per gli analisti:

Procedere come descritto di seguito:

1. Configurazione delle autorizzazioni del livello di accesso per gli analisti di Support Automation (a pagina 1061)
2. Gestione delle code per l'ambiente dell'assistenza in tempo reale (a pagina 1063)
3. Gestione delle notifiche di attività per l'ambiente dell'assistenza in tempo reale (a pagina 1064)

4. Creazione delle impostazioni predefinite di chat per l’ambiente di assistenza (a pagina 1066)
5. Gestione delle attività automatiche per l'ambiente di assistenza in tempo reale (a pagina 1067)

Configurazione delle autorizzazioni del livello di accesso per gli analisti di Support Automation

È possibile configurare i ruoli di CA SDM per le autorizzazioni di Support Automation. Per impostare le autorizzazioni dei ruoli, è sufficiente configurare i livelli di accesso Support Automation per gli analisti e i livelli di riservatezza per gli utenti finali nel proprio ambiente di assistenza in tempo reale.

Sono disponibili i seguenti livelli di accesso:

Analista

Specifica il tipo di contatto che fornisce assistenza in tempo reale agli utenti finali nell'ambiente di supporto. Un livello di accesso definisce le code, le attività automatiche e gli strumenti utilizzabili dall'analista.

Utente finale

Specifica il tipo di contatto che riceve assistenza in tempo reale dagli analisti, come ad esempio un dipendente e un cliente.

È possibile gestire i livelli di accesso Support Automation tramite la scheda Amministrazione.

Procedere come descritto di seguito:

1. Configurare i livelli di accesso appropriati per gli analisti nell'ambiente dell'assistenza in tempo reale. Ad esempio, analista o utente finale.

   È possibile creare livelli di accesso analista per gestire le autorizzazioni degli analisti nel sistema, ad esempio per abilitare o disabilitare strumenti specifici dell'interfaccia Analista Support Automation.

2. Rivedere le informazioni e selezionare i livelli di riservatezza appropriati per gli utenti finali nell'ambiente di assistenza in tempo reale.

   È possibile creare livelli di riservatezza per gestire i livelli di accesso degli utenti finali nel sistema.

3. Assegnare i livelli di accesso ai ruoli È possibile assegnare i livelli di riservatezza degli utenti finali e i livelli di accesso degli analisti a ruoli specifici nel proprio ambiente.

   a. Selezionare Gestione ruoli e protezione, Gestione ruoli, Elenco Ruoli nella scheda Amministrazione.

      Viene visualizzata la pagina Elenco ruoli.

   b. Fare clic sul ruolo a cui si desidera assegnare il livello di accesso; ad esempio Amministratore.

      Viene visualizzata la pagina Dettagli ruolo.

   c. Fare clic su Modifica.

      Viene visualizzata la pagina Aggiorna ruolo.

   d. Nella scheda Autorizzazione selezionare il livello di accesso creato dall'elenco a discesa Accesso SA, quindi fare clic su Salva.

      Viene visualizzata la pagina Dettagli ruolo. Verificare che l'accesso Support Automation sia stato assegnato al ruolo.

      È possibile gestire i livelli di accesso Support Automation e assegnarli a ruoli di CA SDM nell'ambiente di supporto. Tuttavia, poiché le dimensioni e la struttura degli ambienti di supporto variano, è possibile che l'implementazione dei livelli di accesso sia diversa.

      Ad esempio, in un ambiente di supporto di piccole dimensioni, è possibile categorizzare solo uno o due analisti in un singolo livello di accesso. In un ambiente di supporto di dimensioni maggiori, l'amministratore titolare può impostare più livelli di accesso analista e assegnare loro privilegi di accesso e supporto diversi.

Importante: In un ambiente multi-tenancy, gli analisti che non appartengono al fornitore del servizio hanno solo accesso in scrittura al proprio titolare e ai propri titolari secondari. È possibile dare accesso in scrittura di tipo analista ad altri titolari e titolari secondari. Ciò è possibile tramite l'aggiornamento dell'accesso di funzione del titolare a cui si accede per includere i titolari che non sono fornitori del servizio.

Gestione delle code per l'ambiente dell'assistenza in tempo reale

È possibile usare le code per indirizzare le richieste delle sessioni di assistenza all'analista più appropriato. L'utente finale può selezionare una categoria oppure immettere una descrizione del problema del suo computer e i ticket corrispondenti (ad esempio un incidente) vengono indirizzati alla coda appropriata.

Dopo l'installazione iniziale del prodotto, la coda predefinita è Supporto. È possibile impostare più code per semplificare l'ordinamento e il controllo delle diverse richieste di supporto in base alle proprie esigenze aziendali. È tuttavia possibile assegnare solo una coda predefinita a ciascun titolare. Se non si assegna un'impostazione predefinita a una coda titolare oppure se la coda titolare predefinita non è disponibile, il sistema utilizza la coda predefinita pubblica. È possibile impostare l'orario di lavoro per la coda.

Il sistema determina automaticamente dove collocare l'utente finale associando le code alle aree incidente. Se un'area viene associata a una coda, l'utente finale seleziona una categoria e viene indirizzato alla coda appropriata. Le funzionalità di ricerca vengono applicate alla descrizione di un incidente o alla categoria di una questione per individuare le code pertinenti e indirizzare l'utente finale unicamente alla coda adeguata.

Procedere come descritto di seguito:

1. Personalizzare le code per gli analisti e i titolari dell'ambiente dell'assistenza in tempo reale. Per personalizzare la coda, modificare i valori predefiniti del campo e personalizzarli.

   È possibile attivare o disattivare code, chat predefinite impostate, categoria, ore di coda, trasferimenti automatici, nonché specificare le autorizzazioni per titolari e analisti.

2. Selezionare una casella di controllo per assegnare una coda predefinita.

È possibile indirizzare gli utenti finali nella coda predefinita quando inoltrano query che non corrispondono alle code configurate nel proprio ambiente. È possibile anche personalizzare le code per i titolari dell'ambiente.

Nota: se la coda del titolare predefinita non è presente o non è disponibile, viene usata la coda pubblica.

3. Immettere gli orari delle operazioni per le code.

   È possibile gestire le code in base alla disponibilità degli utenti dell'ambiente di supporto, ad esempio abilitando i servizi di Support Automation durante l'orario di lavoro.

   Importante: È possibile assegnare turni sia ai propri orari di Support Automation, sia a singole code di assistenza in tempo reale. L'assegnazione di turni diversi agli orari di Support Automation e alle singole code può causare conflitti per gli analisti e gli utenti finali nell'ambiente di supporto.

Gestione delle notifiche di attività per l'ambiente dell'assistenza in tempo reale

In qualità di amministratori di sistema, è possibile personalizzare le modalità con cui gli utenti finali e gli analisti rilevano e ricevono le notifiche quando si verifica un'attività. Ad esempio, è possibile inviare una notifica quando un analista termina una sessione di assistenza. È possibile creare notifiche di posta elettronica per avvisare gli analisti della presenza di una richiesta di sessione di assistenza nella loro coda.

Selezionare una delle seguenti notifiche predefinite, se non attive, in modo appropriato per l'ambiente:

Notifica voce coda

Informa l'analista quando un utente finale si inserisce in una coda della sessione di assistenza e quando la sessione di assistenza viene trasferita a un'altra coda.

Notifica dell'analista

Segnala all'analista la scadenza del tempo di attesa in coda dell'utente finale. L'evento di scadenza viene identificato utilizzando una macro evento condizionale CA SDM.

Assistenza: invita utente finale ad una sessione - Incidente

Segnala all'utente finale che l'analista ha inviato un invito a partecipare a una sessione di assistenza per un incidente o una richiesta.

Assistenza: invita utente finale ad una sessione - Questione

Segnala all'utente finale che l'analista ha inviato un invito a partecipare a una sessione di assistenza per una questione.

Notifica sessione scaduta

Segnala al sistema il termine di una sessione di assistenza.

Importante: Per utilizzare la funzionalità di Support Automation con un sistema esterno, come Star, per impostazione predefinita il contatto System_SA_User è impostato sulla regola *Notifica sessione scaduta*.

Procedere come descritto di seguito:

1. Accedere ad Amministrazione, Notifica, Notifiche attività.

   Viene visualizzata la pagina Notifiche attività.

2. Selezionare una notifica.

   È possibile utilizzare la notifica selezionata.

Creazione delle impostazioni predefinite di chat per l'ambiente di assistenza

È possibile creare risposte comuni per le domande più frequenti. Anziché immettere più volte la stessa risposta, è possibile salvarla e usarla in altre sessioni chat. Le risposte salvate vengono chiamate chat predefinite.

È possibile inviare automaticamente le chat predefinite, ad esempio un saluto, all'inizio di ciascuna sessione. È possibile anche compilare automaticamente le impostazioni predefinite con informazioni specifiche per la sessione corrente, come il nome dell'analista.

È possibile utilizzare i seguenti tipi di impostazioni predefinite in una sessione di assistenza in tempo reale:

Chat predefinita

Identifica una risposta di testo comunemente usata per una domanda di un utente finale.

URL predefinita

Identifica un URL comunemente usato a cui l'utente finale può accedere.

È possibile localizzare ciascuna impostazione predefinita della chat. L'impostazione predefinita della chat viene sincronizzata con la localizzazione dell'utente finale in modo che riceva le impostazioni predefinite localizzate corrette. È possibile creare usare risposte predefinite per le domande e le situazioni più comuni.

Procedere come descritto di seguito:

1. Esaminare le sessioni di assistenza tipiche della propria organizzazione.
2. Nel menu Support Automation, selezionare Strumenti, Impostazioni predefinite di chat, Elenco Impostazioni predefinite testo.

   Viene visualizzata la pagina Elenco impostazioni predefinite testo di chat.
3. Fare clic su Crea nuovo.

   Viene visualizzata la pagina Crea Nuovo testo predefinito di chat.
4. Inserire i dati nei seguenti campi:

   Titolare

   Specifica il titolare.

   Impostazioni predefinite di chat per Sessione

   Selezionare questa opzione per impostare la configurazione predefinita di chat per Sessione.

   Gruppo di testi predefiniti

   Specifica il gruppo di testi predefiniti.

   Nome del testo predefinito

Specifica il nome del testo predefinito.

Testo predefinito

Specifica il testo dell'impostazione predefinita.

Fare clic su Salva.

Viene creato il testo predefinito di chat.

5. (Facoltativo) Fare clic su Modifica per modificare l'Elenco Testi predefiniti di chat localizzate.

   Viene visualizzata la pagina Aggiorna testo predefinito di chat.

6. Fare clic su un collegamento di localizzazione.

   Viene visualizzata la pagina Dettagli localizzazione del testo predefinito di chat.

7. Fare clic su Modifica.

   Viene visualizzata la pagina Aggiorna Localizzazione testo predefinito di chat.

8. Immettere il nome localizzato e il testo e fare clic su Salva.

   Viene aggiunto il testo localizzato per il testo predefinito di chat.

Gestione delle attività automatiche per l'ambiente di assistenza in tempo reale

È necessario installare e configurare l'editor delle attività automatiche per gestire le attività automatiche usate dagli analisti di Support Automation per fornire supporto agli utenti finali. L'utente può avviare un'attività automatica da un documento della conoscenza e dall'interfaccia self-service oppure l'analista può eseguire un'attività automatica durante una sessione di assistenza. Le attività automatiche offrono agli analisti informazioni dettagliate sul computer dell'utente finale. È possibile creare attività automatiche self-service che interagiscano con l'utente finale ed elaborino il suo input. Queste attività possono modificare il file system, il registro, scaricare software da installare e così via.

Procedere come descritto di seguito:

1. Installare l'editor delle attività automatiche.

   Utilizzare la posizione seguente e avviare il programma di installazione sul supporto di installazione del DVD:

   `casd.nt\SAScriptWriter`

   Nota: Nell'ambiente di supporto è possibile anche copiare e distribuire il programma di installazione agli utenti appropriati. L'editor delle attività automatiche viene installato e si crea un collegamento sul desktop.

2. Fare doppio clic per aprire l'editor delle attività automatiche.

3. Fare clic su Strumenti, Server.

   Viene visualizzata la finestra di dialogo Configurazione server.

4. Immettere il nome host e la porta.

   Impostazione predefinita: 8070

5. Immettere il nome utente e la password di un utente con accesso in lettura o scrittura all'editor delle attività automatiche, come l'analista di Support Automation.

6. Fare clic su Test.

   Lo strumento prova ad accedere all'applicazione di Service Desk con una chiamata di servizi Web e verificare se l'applicazione esiste ed è in grado di accedervi mediante le credenziali.

7. Fare clic su OK.

   Le attività automatiche sono state create e caricate sul server.

   È possibile caricare attività pubbliche o assegnarle a titolari o titolari secondari specifici.

   Importante: Solo i ruoli del titolare Fornitore del servizio con il flag Aggiorna oggetti pubblici abilitato possono caricare le attività e le librerie sul server. Tutto il contenuto della libreria delle attività e il contenuto statico vengono memorizzati come dati pubblici.

La configurazione viene completata e gli analisti possono utilizzarla per aiutare gli utenti. Gli analisti di Support Automation controllano e gestiscono più richieste degli utenti finali nel corso di sessioni di assistenza in tempo reale. Gli analisti utilizzano gli strumenti di Support Automation per interagire con gli utenti finali e fornire loro assistenza in tempo reale. Possono accedere all'interfaccia tramite un ticket di CA SDM, come un incidente, o tramite la scheda di Support Automation per avviare una sessione.

Avvio dell'Assistenza in tempo reale da parte degli analisti

Gli analisti possono avviare l'Assistenza in tempo reale come segue:

1. L'analista può effettuare una *qualsiasi* delle seguenti operazioni:
   - Accedere a CA SDM e selezionare la scheda Automazione supporto.
   - Aprire un ticket CA SDM e selezionare la scheda Automazione supporto.
2. CA SDM richiede all'analista di installare la versione 1.6 o successiva di Java Runtime Environment (JRE), se non ancora stata installata. L'Interfaccia Analista di Support Automation non supporta JRE a 64 bit.

   Nota: il browser Safari richiede JRE 1.6.0_30 a 32 bit, o versione successiva.

   CA SDM avvia l'interfaccia Analista Support Automation.

Nota: la tabella sa_login_session crea un record ogni volta che l'analista avvia l'interfaccia Analista Support Automation e quando utente finale avvia il client Web. Per ulteriori informazioni sulla tabella sa_login_session, consultare la *Guida di riferimento tecnico* di *CA SDM*.

Configurazione delle opzioni di connessione Java

È possibile configurare le opzioni di connessione Java per nel caso in cui l'interfaccia Analista Support Automation non sia in grado di connettersi al server Support Automation. Questo problema si verifica quando la configurazione predefinita del browser dell'analista non è stata impostata correttamente per l'ambiente e non è in grado di avviare Assistenza in diretta. È possibile modificare le impostazioni di connessione dell'analista utilizzando un browser o il Pannello di controllo di Java.

Per configurare le opzioni di connessione nel browser:

1. Aprire il browser Web; ad esempio Internet Explorer.

   Il browser si apre.

2. Fare clic su Strumenti, Opzioni Internet.

   Viene visualizzata la finestra di dialogo Opzioni Internet.

3. Configurare le impostazioni di connessione appropriate, come una connessione diretta o un server proxy.
4. Fare clic su OK.

   Vengono configurate le aperture della configurazione.

Per configurare le opzioni di connessione nel Pannello di controllo di Java:

1. Aprire il Pannello di controllo di Java utilizzando il comando:

   ```
   javaws -viewer
   ```

   Viene visualizzato il Pannello di controllo di Java.

2. Nella scheda General, fare clic su Network Settings.

   Viene visualizzata la finestra di dialogo Network Settings.

3. Configurare le impostazioni appropriate, come una connessione diretta o un server proxy.

   Fare clic su OK.

   Vengono configurate le aperture della configurazione.

Come configurare Assistenza in tempo reale per gli analisti

Per configurare l'interfaccia Analista di automazione supporto definendo autorizzazioni per i ruoli e la protezione per gli analisti del proprio ambiente di assistenza in tempo reale, effettuare le seguenti operazioni:

1. Creare o modificare i ruoli (a pagina 1074) e i livelli di accesso Support Automation (a pagina 1079) appropriati per gli analisti del proprio ambiente di assistenza in tempo reale

   È possibile aggiornare i ruoli e i livelli di accesso per assegnare agli analisti l'autorizzazione ad accedere agli strumenti specifici da utilizzare durante le sessioni di assistenza.

2. Definire e gestire le code (a pagina 1084) per il proprio ambiente di assistenza in tempo reale

   È possibile creare code per indirizzare in modo appropriato le richieste di assistenza in tempo reale in arrivo.

3. Definire e gestire le notifiche attività (a pagina 1080) per il proprio ambiente di assistenza in tempo reale

   È possibile creare notifiche di posta elettronica per avvisare gli analisti della presenza di una richiesta di sessione di assistenza nella loro coda.

4. Definire e gestire le preimpostazioni chat (a pagina 1096) per il proprio ambiente di assistenza in tempo reale

   È possibile creare preimpostazioni chat per consentire agli utenti di inviare risposte preconfigurate alle domande più frequenti e nelle situazioni più comuni.

5. Definire e gestire le attività automatiche per il proprio ambiente di assistenza in tempo reale

   È possibile creare attività automatiche per eseguire azioni specifiche sul computer dell'utente finale.

   Nota: è possibile creare script e caricarli sul server solo tramite l'editor delle attività automatiche IDE.

Procedure utilizzabili dagli utenti finali per accedere alle sessioni di assistenza

L'utente finale richiede le sessioni di assistenza tramite la pagina iniziale CA SDM oppure rivolgendosi direttamente all'help desk per telefono o tramite posta elettronica. L'analista Support Automation invita l'utente finale ad accedere a una sessione utilizzando il ticket CA SDM.

1. L'utente finale può effettuare una *qualsiasi* delle seguenti operazioni:

   - Richiedere sessioni chat in tempo reale tramite la pagina iniziale CA SDM.

     Viene visualizzata la pagina Avvia chat live che chiede all'utente finale di immettere un'area incidente e una descrizione. L'utente finale seleziona Continua, la sessione si apre e l'utente finale viene inserito nella coda appropriata.

   - A questo punto l'utente finale seleziona il collegamento contenuto nella notifica ricevuta per posta elettronica e accede alla sessione di assistenza utilizzando le credenziali e il codice di accesso alla sessione forniti dall'analista.

     Se l'utente usa la notifica ricevuta per posta elettronica, la coda viene ignorata.

   - A questo punto seleziona Contatta analista e immette il codice di accesso alla sessione per ignorare la coda.

     Nota: all'avvio del client Support Automation dell'utente finale, viene scaricato un file eseguibile per l'avvio del programma. L'avvio deve essere effettuato manualmente dall'utente finale. Tuttavia, per motivi di sicurezza, l'utente finale deve avviare il file eseguibile entro un determinato limite di tempo. Alla scadenza di questo intervallo di tempo, viene visualizzato un messaggio di errore sul computer dell'utente finale al momento in cui tenta di avviare il file eseguibile del programma di avvio.

2. L'analista fornisce assistenza in tempo reale all'utente remoto tramite una sessione chat. L'utente finale può utilizzare il proprio browser Web per la chat con l'analista oppure avviare il file eseguibile dell'agente.

   Nota: se l'analista non è in grado di risolvere la sessione utilizzando WebChat, può invitare l'utente finale a usare gli strumenti completi disponibili nell'interfaccia Analista di automazione supporto utilizzando la finestra Sessione analista. L'utente finale deve accettare la richiesta per avviare il client sul computer e per consentire all'analista di usare questi strumenti.

Procedure usate dagli analisti per automatizzazione il supporto per gli utenti finali

Gli analisti utilizzano gli strumenti Assistenza in tempo reale per eseguire le seguenti attività sui computer degli utenti finali:

- Effettuare sessioni di conversazioni in tempo reale host
- Visualizzare i file system
  - Creare, modificare, rinominare o eliminare file e directory
  - Copiare e trasferire file e cartelle al computer dell'utente finale
- Visualizzare i registri di sistema
  - Creare, modificare o eliminare record del registro
  - Esportare o importare valori del registro dal registro dell'utente finale
- Acquisire di schermate dal computer dell'utente finale nel caso in cui la qualità della connessione non sia sufficiente per l'assistenza con controllo remoto
- Visualizzare il computer desktop dell'utente finale
- Controllare remotamente il computer dell'utente finale
- Avviare un programma sul computer dell'utente finale
- Riavviare o spegnere il computer dell'utente finale
- Esecuzione di attività automatiche

Nota: per informazioni dettagliate sulle modalità di utilizzo degli strumenti Assistenza in tempo reale da parte degli analisti, consultare la *Guida in linea*.

Ulteriori informazioni:

Amministrazione livello di accesso Support Automation (a pagina 1079)

Procedure utilizzate dagli analisti per fornire assistenza in tempo reale

Gli analisti forniscono assistenza in tempo reale agli utenti finali utilizzando l'interfaccia Analista di automazione supporto. Gli analisti gestiscono gli utenti finali indirizzati alle loro code, gestiscono le sessioni di assistenza e partecipano alle sessioni alle quali sono autorizzati ad accedere.

1. L'utente finale richiede una sessione di assistenza tramite la pagina iniziale CA SDM o un ticket, come un Incidente, una Richiesta o una Issue.
2. L'utente finale si connette a una coda.

   Nota: se l'utente finale si connette a una sessione utilizzando il collegamento contenuto nell'invito inviato per posta elettronica dall'analista, ignora la coda.

   È possibile configurare le aree delle Richiesta e le categorie delle Issue CA SDM per l'indirizzamento degli utenti alle code.
3. L'analista seleziona l'utente finale dalla coda.
4. La sessione di assistenza si avvia e l'analista fornisce assistenza in tempo reale.

   Nota: se l'analista avvia l'interfaccia Analista di automazione supporto tramite la scheda Automazione supporto, non viene associato alcun ticket CA SDM alla sessione di assistenza.
5. L'analista crea il ticket al momento in cui chiude la sessione di assistenza e imposta lo stato come *SA-Apri* o *SA-Risolto*, oppure trasferisce la sessione di assistenza a un'altra coda.
6. L'analista chiude la sessione e l'utente finale riceve una notifica per posta elettronica con il registro sessione.

Nota: per informazioni dettagliate sulle modalità usate dagli analisti per gestire le code e le sessioni di assistenza, consultare la *Guida in linea*.

Amministrazione degli utenti Support Automation

Gli amministratori del sistema e gli amministratori titolari possono configurare contatti CA SDM, autorizzazioni per i ruoli, livelli di accesso e di riservatezza per definire le autorizzazioni utente. Di seguito vengono elencati gli utenti che utilizzano Support Automation.

Amministratore del sistema

Accesso a livello di sistema che consente di aggiungere e modificare tutte le impostazioni predefinite e Support Automation predefinite e le funzioni nella scheda Amministrazione. L'amministratore del sistema ha il compito di impostare titolari e analisti, personalizzare le proprietà di sistema Support Automation e reimpostare le password di sistema.

Amministratore titolari

Definisce i diritti amministrativi a livello di titolare, ma non consente di creare o modificare altri titolari o di reimpostare le password degli utenti. Le autorizzazioni vengono determinate dal titolare del fornitore del servizio.

Analista

Definisce i diritti per l'utente che fornisce assistenza in tempo reale agli utenti finali nell'ambiente di supporto.

Utente finale

Definisce i diritti per gli utenti che possono richiedere assistenza in tempo reale agli analisti dell'ambiente di supporto, come i dipendenti e i clienti.

Configurazione delle autorizzazioni dei ruoli Support Automation

È possibile configurare i ruoli CA SDM con autorizzazioni Support Automation. Per impostare le autorizzazioni per i ruoli, è sufficiente configurare i livelli di accesso Support Automation per gli analisti e i livelli di riservatezza per gli utenti finali nel proprio ambiente di assistenza in tempo reale, come indicato di seguito:

1. Configurare i livelli di accesso per gli analisti appropriati nell'ambiente di assistenza in tempo reale

   È possibile creare livelli di accesso analista per gestire le autorizzazioni degli analisti nel sistema; ad esempio per abilitare o disabilitare strumenti specifici dell'interfaccia Analista Support Automation.

2. Configurare i livelli di riservatezza per gli utenti finali appropriati nell'ambiente di assistenza in tempo reale

   È possibile creare livelli di riservatezza per gestire i livelli di accesso degli utenti finali nel sistema.

3. Assegnare (a pagina 1080) i livelli di accesso ai ruoli

   È possibile assegnare i livelli di riservatezza degli utenti finali e i livelli di accesso degli analisti a ruoli specifici nel proprio ambiente.

Nota: per informazioni dettagliate sulla creazione e modifica dei livelli di accesso Support Automation per gli analisti e la configurazione dei livelli di protezione per gli utenti finali, consultare la *Guida in linea*.

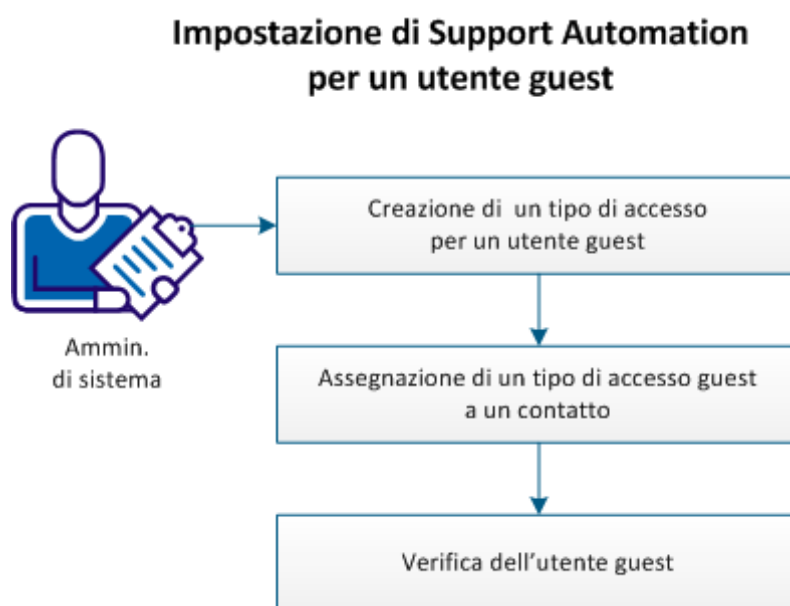
Utenti anonimi e registrati Support Automation

Il server Support Automation è in grado di accettare utenti registrati e anonimi, a seconda delle autorizzazioni CA SDM. Se l'operazione è consentita, l'utente guest permette agli utenti anonimi di connettersi a CA SDM. È possibile autenticarsi sul server per accedere a:

- Assistenza in tempo reale
- Self-service
- Editor delle attività automatiche
- Client End-User

Configurazione di Support Automation per un utente guest

In qualità di amministratori di sistema, è possibile configurare l'ambiente di assistenza in tempo reale per consentire agli utenti guest di interagire con gli analisti. È possibile configurare un utente guest per un titolare specifico oppure rendere l'utente disponibile per il sistema intero. Il titolare è un utente che utilizza un'istanza singola di un'applicazione software che serve più clienti in un ambiente multi-tenancy.

Il diagramma seguente illustra la configurazione dell'ambiente dell'assistenza in tempo reale, eseguita da un amministratore di sistema, per permettere agli utenti guest le attività seguenti:

Procedere come descritto di seguito:

1. Creazione di un tipo di accesso per un utente guest (a pagina 1077)
2. Assegnazione del tipo di accesso guest a un contatto (a pagina 1078)
3. Verifica dell'utente guest (a pagina 1078)

Creazione di un tipo di accesso per un utente guest

Per consentire agli utenti guest l'accesso a CA SDM senza autenticazione, creare un tipo di accesso specifico in CA SDM. Il fornitore del servizio può creare un tipo di accesso guest per ciascun titolare dell'ambiente.

Procedere come descritto di seguito:

1. Accedere a CA SDM.
2. Nella scheda Amministrazione, fare clic su Gestione protezione e ruoli, Tipi di accesso.

   Viene visualizzata la pagina Elenco Tipi accesso.
3. Fare clic su Crea Nuovo.

   Viene visualizzata la pagina Crea nuovo tipo di accesso.
4. Compilare i campi in modo appropriato.
5. Fare clic sulla scheda Autenticazione Web. Nell'elenco a discesa Tipo validazione, selezionare Apertura - Consenti sempre accesso.
6. Fare clic su Salva.

   Il tipo di accesso per gli utenti guest è stato creato.
7. (Facoltativo) Fare clic con il pulsante destro del mouse sulla pagina di Elenco Tipi accesso e selezionare Aggiorna.

   Il tipo di accesso guest viene visualizzato nell'elenco.

Assegnazione del tipo di accesso guest a un contatto

Assegnare il tipo di accesso guest a un contatto dopo aver creato un tipo di accesso in modo che l'utente guest possa utilizzare la funzionalità di assistenza in tempo reale di Support Automation. L'utente guest utilizza l'autenticazione Web per accedere a CA SDM. Un contatto è una persona che utilizza il sistema regolarmente.

Procedere come descritto di seguito:

1. Nella scheda Amministrazione, fare clic su Gestione protezione e ruoli, Contatti.

   Viene visualizzata la pagina Ricerca contatto.

2. Fare clic su Crea Nuovo.

   Viene visualizzata la pagina Crea Nuovo contatto.

   Nota: è possibile anche modificare un contatto.

3. Selezionare Guest dall'elenco a discesa Tipo contatto.
4. (Facoltativo) Associare il contatto a un titolare e rendere pubblico il contatto. Questa associazione permette ai contatti di accettare l'assegnazione automatica di una richiesta.
5. Fare clic su Salva.

   Il tipo di accesso Guest viene assegnato al contatto.

Verifica dell'utente guest

Dopo aver assegnato il tipo di accesso, è possibile verificare l'esistenza degli utenti appropriati nell'ambiente.

Procedere come descritto di seguito:

1. Nella scheda Amministrazione, fare clic su Gestione protezione e ruoli, Contatti.

   Viene visualizzata la pagina Ricerca contatto.

2. Selezionare Guest come Tipo contatto e il tipo di accesso assegnato.
3. Fare clic su Cerca.

   Viene visualizzata la pagina Elenco Contatti.

I tipi di contatto e di accesso sono disponibili nella pagina Elenco Contatti.

Questa fase completa l'installazione di Support Automation per un utente guest.

Amministrazione livello di accesso Support Automation

È possibile gestire i livelli di accesso Support Automation e assegnarli a ruoli CA SDM nell'ambiente di supporto. Tuttavia, poiché le dimensioni e la struttura degli ambienti di supporto variano, è possibile che l'implementazione dei livelli di accesso sia diversa.

In un ambiente di supporto di piccole dimensioni, è possibile categorizzare solo uno o due analisti in un singolo livello di accesso come Analista. In un ambiente di supporto di dimensioni maggiori, l'amministratore titolare può impostare più livelli di accesso analista e assegnare loro privilegi di accesso e supporto diversi.

Importante. In un ambiente Multi-Tenancy, gli analisti che non appartengono al fornitore del servizio hanno solo accesso in scrittura al proprio titolare e ai propri sottotitolari. È possibile assegnare l'accesso in scrittura analista ad altri titolari e sottotitolari aggiornando l'accesso alle funzioni del titolare a cui si ha accesso in modo che includa i titolari che non appartengono al fornitore del servizio.

Sono disponibili i seguenti livelli di accesso:

Analista

Specifica il tipo di contatto che fornisce assistenza in tempo reale agli utenti finali nell'ambiente di supporto. I livelli di accesso specificano quali code, attività automatiche e strumenti possono essere usati dall'analista.

Utente finale

Specifica il tipo di contatto che riceve assistenza in tempo reale dagli analisti; ad esempio un dipendente e cliente.

È possibile gestire i livelli di accesso Support Automation tramite la scheda Amministrazione.

Nota: per informazioni dettagliate sulla creazione e modifica dei livelli di accesso Support Automation per gli analisti e gli utenti finali, consultare la *Guida in linea*.

Assegnazione di un livello di accesso a un ruolo

È possibile assegnare livelli di accesso Support Automation ai ruoli CA SDM esistenti nel proprio ambiente.

Per assegnare un livello di accesso a un ruolo:

1. Selezionare Gestione ruoli e protezione, Gestione ruoli, Elenco Ruoli nella scheda Amministrazione.

   Viene visualizzata la pagina Elenco ruoli.

2. Fare clic sul ruolo a cui si desidera assegnare il livello di accesso; ad esempio Amministratore.

   Viene visualizzata la pagina Dettagli ruolo.

3. Fare clic su Modifica.

   Viene visualizzata la pagina Aggiorna ruolo.

4. Nella scheda Autorizzazione selezionare il livello di accesso creato dall'elenco a discesa Accesso SA, quindi fare clic su Salva.

   Viene visualizzata la pagina Dettagli ruolo. Verificare che l'accesso Support Automation sia stato assegnato al ruolo.

Amministrazione delle notifiche relative all'attività di Support Automation

È possibile utilizzare le notifiche attività per gestire le attività Support Automation. Ad esempio è possibile personalizzare la modalità con cui gli utenti finali, gli analisti e gli amministratori tengono traccia e ricevono le notifiche quando si verifica un'attività specifica, come il termine di una sessione di assistenza.

Le seguenti notifiche predefinite possono essere personalizzate in base alle esigenze del proprio ambiente:

Notifica voce coda

Segnala all'analista quando un utente finale accede alla coda di una sessione di assistenza.

Segnala all'analista quando la sessione di assistenza viene trasferita a un'altra coda.

Notifica dell'analista

Segnala all'analista la scadenza del tempo di attesa in coda dell'utente finale. L'evento di scadenza viene identificato utilizzando una macro evento condizionale CA SDM.

Assistenza: invita utente finale ad una sessione - Incidente

Segnala all'utente finale che l'analista ha inviato un invito a partecipare a una sessione di assistenza da un Incidente o una Richiesta.

Assistenza: invita utente finale ad una sessione - Issue

Segnala all'utente finale che l'analista ha inviato un invito a partecipare a una sessione di assistenza da una Issue.

Notifica sessione scaduta

Segnala al sistema il termine di una sessione di assistenza.

Importante. Per utilizzare la funzionalità Support Automation con un sistema esterno, come Star, per impostazione predefinita è necessario impostare il contatto System_SA_User sulla regola *Notifica sessione scaduta*.

Adattamenti pagine Support Automation

È possibile configurare l'aspetto delle pagine Support Automation per gli utenti finali in base alle proprie esigenze aziendali. I seguenti adattamenti consentono di specificare ciò che vede l'utente prima di connettersi a una sessione di assistenza e al termine della sessione:

- Personalizzazione dell'intestazione e del piè di pagina di tutte le pagine visibili all'utente finale

  È possibile modificare il codice HTML dell'intestazione e del piè di pagina nonché modificare anche l'ubicazione del file CSS che contiene le definizioni degli stili.

- Personalizzazione delle esigenze di localizzazione dell'ambiente

  È possibile impostare le impostazioni internazionali predefinite per gli analisti e gli utenti finali.

- Personalizzazione dei layout di pagina visibili agli utenti al momento dell'accesso e in attesa di connettersi a sessioni di assistenza

  È possibile personalizzare le pagine che indirizzano gli utenti finali in base alle proprie esigenze aziendali.

Nota: per informazioni più dettagliate sulla configurazione delle pagine Support Automation per gli analisti e gli utenti finali, consultare la *Guida in linea*.

Amministrazione personalizzazione

È possibile personalizzare l'intestazione e il piè di pagina delle pagine presentate all'utente finale, come self-service. È possibile modificare il codice HTML dell'intestazione e del piè di pagina nonché modificare anche l'ubicazione del file CSS che contiene le definizioni degli stili.

È possibile visualizzare un elenco di record personalizzati fino a un massimo di un elenco per ciascun titolare. I titolari possono creare personalizzazioni oppure, se l'opzione di personalizzazione non è stata definita per il titolare, usare le impostazioni di sistema predefinite. È possibile anche abilitare la localizzazione delle personalizzazioni e visualizzare un elenco di tutte le personalizzazioni localizzate per le localizzazioni abilitate.

Importante Le personalizzazioni da CA Support Automation r6,0 SR1 eFix5 non migrano automaticamente a CA SDM Versione 12.9. Si consiglia di controllare la personalizzazione per verificare che corrisponda alla personalizzazione CA SDM. Se necessario, copiare e incollare i dati relativi a intestazione, piè di pagina e URL CSS di ciascuna divisione nel titolare (o pubblico) corrispondente in CA SDM per la migrazione dei dati di personalizzazione.

Amministrazione della localizzazione

La localizzazione permette di supportare più lingue contemporaneamente nella stessa installazione grazie alla possibilità di tradurre gli elementi dell'applicazione in una lingua specifica. Questi elementi possono includere messaggi di sistema, icone e contenuto. Le informazioni vengono visualizzate nel miglior formato per l'utente, indipendentemente dalla lingua nativa.

Le versioni localizzate di Support Automation sono in grado di soddisfare le esigenze di un ambiente globale. Ciascun titolare può gestire più lingue e le localizzazioni possono essere applicate a più titolari. Ciascun titolare condivide le impostazioni di sistema predefinite con la propria localizzazione. È possibile configurare la lingua per l'utente finale e l'analista prima di avviare Assistenza in tempo reale utilizzando l'elenco di lingue abilitate. L'analista può usare una lingua diversa rispetto a quella dell'utente durante una sessione di assistenza.

È possibile modificare il testo localizzato per le esclusioni di responsabilità. Non è possibile creare o rimuovere localizzazioni, ma solo abilitarle o disabilitarle.

Nota: l'interfaccia dell'amministratore è disponibile solo nella localizzazione server predefinita.

Configurazione del layout della pagina

Quando un utente accede ad Assistenza in tempo reale da CA SDM, vede una pagina di avvio predefinita. Allo stesso modo, quando viene inizialmente messo in attesa in una coda, vede nuovamente una pagina predefinita.

Se non si specificano impostazioni speciali per i titolari, vengono utilizzate le impostazioni pubbliche predefinite. È possibile configurare le seguenti impostazioni pubbliche per le code che non hanno impostazioni specifiche:

- Pagina di attesa:
- Pagina di post-avvio per l'utente finale
- In Sessione
- Pagina post disconnessione
- Pagina di uscita indagine

Ciascuna pagina ha una pagina Dettagli che comprende un campo di testo per l'immissione dell'URL e una casella di controllo per contrassegnare la pagina come esterna.

Proprietà di sistema Support Automation

È possibile personalizzare, rispetto all'installazione predefinita, molte delle modalità in cui Support Automation gestisce le attività. È possibile usare le impostazioni predefinite delle opzioni di sistema per personalizzare il comportamento di Support Automation. È possibile personalizzare ad esempio alcune delle seguenti opzioni Support Automation:

- Abilitare o disabilitare il collegamento per la chat in tempo reale tramite la pagina iniziale dei dipendenti e clienti CA SDM.
- Abilitare o disabilitare il collegamento per la partecipazione a una sessione tramite la pagina iniziale dei dipendenti e clienti CA SDM.
- Abilitare o disabilitare l'opzione per creare un incidente CA SDM quando l'utente finale si disconnette mentre è nella coda di Support Automation in attesa del suo turno.

Le proprietà di sistema sono opzionali per il titolare. Se un titolare non ha definito le sue proprietà, Support Automation utilizza le impostazioni pubbliche (condivise). L'installazione del prodotto crea le proprietà pubbliche predefinite.

Nota:per ulteriori informazioni su come configurare le proprietà di sistema Support Automation, consultare la *Guida in linea*.

Amministrazione delle code Support Automation

È possibile usare le code per indirizzare le richieste delle sessioni di assistenza all'analista più appropriato. L'utente finale può selezionare una categoria oppure immettere una descrizione del problema del suo computer e i ticket corrispondenti (ad esempio un incidente) viene indirizzato alla coda appropriata.

Dopo l'installazione iniziale del prodotto, la coda predefinita è Supporto. È possibile impostare più code per semplificare l'ordinamento e il controllo delle diverse richieste di supporto in base alle proprie esigenze aziendali. È tuttavia possibile assegnare solo una coda predefinita a ciascun titolare. Se non si assegna un'impostazione predefinita a una coda titolare oppure se la coda titolare predefinita non è disponibile, il sistema utilizza la coda predefinita pubblica. È possibile impostare l'orario di lavoro per la coda.

Il sistema determina automaticamente dove collocare l'utente finale associando le code alle aree incidente. Se un'area viene associata a una coda, l'utente finale seleziona una categoria e viene indirizzato alla coda appropriata. Le funzionalità di ricerca vengono applicata alla descrizione di un Incidente o alla categoria di una Questione per individuare le code pertinenti e indirizzare l'utente unicamente alla coda adeguata.

Nota: per informazioni più dettagliate sulla personalizzazione e il mapping delle code Support Automation, consultare la *Guida in linea*.

Gestione delle code

È possibile configurare code per permettere agli utenti finali di ricevere un'assistenza in tempo reale appropriata dagli analisti. È inoltre possibile gestire le code per migliorare l'indirizzamento degli utenti alle sessioni di assistenza effettuando le seguenti operazioni:

- Personalizzazione delle code per gli analisti e i titolari dell'ambiente di assistenza in diretta

  È possibile attivare o disattivare code e specificare autorizzazioni per il titolare e l'analista.

- Assegnazione di una coda predefinita

È possibile inviare gli utenti finali nella coda predefinita quando inoltrano query che non corrispondono alle code configurate nel proprio ambiente. È possibile anche personalizzare le code per i titolari dell'ambiente.

Nota: se la coda del titolare predefinita non è presente o non è disponibile, viene usata la coda pubblica.

- Assegnazione di orari alle code

  È possibile gestire le code in base alla disponibilità degli utenti dell'ambiente di supporto; ad esempio abilitando i servizi Support Automation durante l'orario di lavoro.

  Importante. È possibile assegnare turni sia ai propri orari Support Automation sia a code di assistenza in tempo reale individuali. L'assegnazione di turni diversi agli orari di Support Automation e alle code individuali può causare conflitti per gli analisti e gli utenti finali nell'ambiente di supporto.

Gestione dei riepiloghi di coda

È possibile comporre i campi visualizzati dall'analista nella pagina di riepilogo delle code. È possibile selezionare un'opzione dal seguente set di campi per il riepilogo delle code, ma non creare nuovi campi:

- Coda
- Domanda
- Tempo di attesa
- Posta elettronica
- Azienda
- Indirizzo IP
- Analista assegnatario
- Categoria
- Lingua
- Titolare

Ulteriori informazioni:

Gestione delle code (a pagina 1084)
Gestione delle ore delle code (a pagina 1086)

Gestione delle ore delle code

È possibile abilitare Support Automation per ciascuna coda a ore specifiche del giorno per adattare l'orario di lavoro degli analisti effettuando le seguenti operazioni:

- Creare una pianificazione separata per ciascuna coda e per tutti i servizi di supporto automatici.

  Nota: queste impostazioni non limitano in alcun modo le funzioni self-service.

- Definire le ore di supporto per il server di Support Automation utilizzando uno stato globale aperto o chiuso. La presenza di una voce per ciascuna ora della settimana indica una differenza rispetto allo stato globale del server.
- Il server utilizza la prima voce di ciascuna ora in base alle regole definite.

  Questa azione consente di unire efficacemente le definizioni delle ore del supporto utilizzando le impostazioni del titolare (o pubbliche) padre. Questa azione potrebbe avere effetti controproducenti se si utilizza una combinazione di stati 'predefinito-chiuso' e 'predefinito-aperto' nella gerarchia.

Gestione dei modelli di ticket

È possibile specificare quali modelli di ticket sono disponibili per l'interfaccia utente analista. È possibile selezionare i modelli di ticket per i tipi di ticket Incidente/Richiesta e Questione.

È possibile definire se il ticket è predefinito o attivo. Quando si crea un modello di ticket è possibile scegliere tra modelli CA SDM esistenti. Il modello predefinito deve essere attivo.

Per ogni titolare, un solo modello di ticket può essere selezionato come predefinito.

Nota: per informazioni più dettagliate su come personalizzare i modelli dei ticket, consultare la *Guida in linea*.

Impostazioni di amministrazione

È possibile definire e configurare le seguenti impostazioni Support Automation:

- Server messaggio di routing
- Autorizzazioni utente finale (livelli di riservatezza)
- Orario Support Automation

Configurazione delle impostazioni Support Automation

È possibile configurare le impostazioni Support Automation dell'ambiente di supporto in base alle proprie esigenze aziendali. Le impostazioni consentono di controllare le funzionalità amministrative, come i server di indirizzamento dei messaggi, i livelli di riservatezza e l'orario Support Automation.

- La configurazione dei server di indirizzamento dei messaggi consente di migliorare le prestazioni durante le sessioni di assistenza.

  È possibile collegare gli utenti finali al server locale preferito dell'analista oppure al server principale predefinito nel caso in cui la connessione non possa essere stabilita.

- È possibile definire livelli di sicurezza per gli utenti finali del proprio ambiente.

  È possibile abilitare strumenti specifici dell'interfaccia Analista Support Automation in base ai livelli di riservatezza usati nel proprio ambiente.

- È possibile impostare l'orario Support Automation su un orario specifico oppure come sempre aperto.

  È possibile indirizzare le richieste di assistenza in tempo reale quando il supporto tecnico è chiuso, ad esempio aprendo una pagina Web che fornisca all'utente l'orario del supporto tecnico e opzioni di supporto aggiuntive.

Nota:per ulteriori informazioni su come configurare le impostazioni Support Automation, consultare la *Guida in linea*.

Server messaggio di routing

È possibile utilizzare Server messaggio di routing (MRS) per gestire diversi server di controllo remoto, in base alla posizione geografica del server locale. L'utilizzo di MRS consente di ottenere prestazioni migliori durante le sessioni di assistenza. Quando si abilita MRS, l'interfaccia Analista Support Automation e il client dell'utente finale tentano di connettersi al server analista preferito (locale) per la condivisione. Se non è possibile eseguire la connessione, la sessione di condivisione torna al server predefinito principale. Il registro in tempo reale registra quale MRS si usa durante la sessione di assistenza.

È possibile creare, aggiornare, rimuovere, abilitare o disabilitare l'oggetto Server messaggio di routing.

Nota:per ulteriori informazioni su come configurare i server messaggi di routing, consultare la *Guida in linea*.

Livelli di riservatezza Support Automation

I livelli di riservatezza vengono utilizzati per impostare il tipo di azioni consentite relative a diversi utenti finali, allo scopo di proteggerne la privacy. I livelli di riservatezza sono associati ai ruoli CA SDM. Sono disponibili tre autorizzazioni predefinite: alta, media e bassa. Ma è possibile definirne di ulteriori se necessario. È possibile aggiungere, aggiornare ed eliminare i livelli di riservatezza disponibili per l'utente finale.

È possibile impostare il nome e la descrizione del livello di riservatezza. È possibile definire quali funzioni degli strumenti specificati (Esplorazione file, Registro remoto, Esegui programma e così via) sono abilitati per il livello di riservatezza abilitato.

Nota:per ulteriori informazioni su come configurare i livelli di riservatezza Support Automation, consultare la *Guida in linea*.

Orari Support Automation

È possibile impostare Support Automation in modo che operi in orari specifici o costantemente. Gli orari di servizio saranno gestiti in base alle esigenze degli utenti finali nel proprio ambiente di supporto. Gli utenti non possono accedere a Support Automation quando è chiuso. È possibile apportare rapide modifiche a diversi turni in una sola operazione.

Importante. È possibile assegnare turni sia ai propri orari Support Automation sia a code di assistenza in tempo reale individuali. L'assegnazione di turni diversi agli orari di Support Automation e alle code individuali può causare conflitti per gli analisti e gli utenti finali nell'ambiente di supporto.

Nota:per ulteriori informazioni su come configurare gli orari Support Automation, consultare la *Guida in linea*.

Personalizzazione degli strumenti Support Automation

È possibile configurare gli strumenti Support Automation dell'ambiente di supporto in base alle proprie esigenze aziendali. Le impostazioni consentono di definire le funzionalità amministrative, come le attività automatiche, le preimpostazioni chat, le credenziali predefinite e le dichiarazioni di responsabilità.

- È possibile personalizzare l'elenco delle attività automatiche e le classificazioni utilizzate dagli analisti Support Automation per fornire supporto agli utenti finali.
- È anche possibile configurare preimpostazioni chat per le risposte comuni alle domande e situazioni più frequenti.
- La configurazione delle credenziali predefinite consente di accedere al computer di un utente finale.
- È possibile personalizzare le dichiarazioni di responsabilità che l'utente vede prima di avviare attività self-service.

Nota:per ulteriori informazioni su come configurare gli strumenti Support Automation, consultare la *Guida in linea*.

Attività automatiche

Un'*attività automatica* è una raccolta di passaggi che definiscono un processo automatico seguito dall'analista o da un utente finale. I passaggi delle attività automatiche sono routine scritte in VBScript o JavaScript che eseguono azioni specifiche sul computer dell'analista o dell'utente finale. È possibile creare nuove attività automatiche e passaggi delle attività mediante l'Automated Task Editor (Editor attività automatizzate). Le routine più comuni comprendono la raccolta di informazioni di telemetria, la diagnosi dei problemi e l'implementazione delle risoluzioni.

Quando si esegue un'attività automatica, il registro viene aggiornato. Questo registro è collegato ed accessibile dal registro sessione di assistenza. Le voci nel registro delle attività automatiche comprendono una serie di voci di testo con data e ora. Queste voci possono essere create richiamando Functions.LogMessage() o WScript.Echo().

Ulteriori informazioni:

Modalità di implementazione delle attività automatiche (a pagina 1091)

Modalità di configurazione delle attività automatiche

È possibile installare e configurare l'editor delle attività automatiche per gestire le attività automatiche usate dagli analisti Support Automation per fornire supporto agli utenti finali. L'utente può avviare un'attività automatica da un documento della conoscenza e dall'interfaccia self-service oppure l'analista può eseguire un'attività automatica durante una sessione di assistenza. Le attività automatiche offrono agli analisti informazioni dettagliate sul computer dell'utente finale. È possibile creare attività automatiche self-service che interagiscano con l'utente finale ed elaborino il suo input. Queste attività possono modificare il file system, il registro, scaricare software da installare e così via. Per configurare le attività automatiche, effettuare le seguenti operazioni:

1. Installare l'editor delle attività automatiche.

   Avviare il programma di installazione dalla seguente ubicazione sul supporto di installazione:

   ```
   casd.nt\SAScriptWriter
   ```

   Nota: è possibile anche copiare il programma di installazione e distribuirlo agli utenti appropriati nel proprio ambiente di supporto.

   L'editor delle attività automatiche viene installato.

2. Aprire l'editor delle attività automatiche.

   Il programma di installazione dell'editor delle attività automatiche crea un collegamento sul desktop.

3. Impostare i seguenti parametri di connessione:

   a. Fare clic su Strumenti, Server.

      Viene visualizzata la finestra di dialogo Configurazione server.

   b. Immettere il nome host e la porta.

      Porta predefinita: 8070

   c. Immettere il nome utente e la password di un utente con accesso in lettura/scrittura all'editor delle attività automatiche, come l'analista Support Automation.

   d. Fare clic su Test.

   e. Fare clic su OK.

4. Creare le attività automatiche e caricarle sul server.

   È possibile caricare attività pubbliche oppure assegnarle a titolari o sottotitolari specifici.

   Importante. Solo i ruoli del titolare Fornitore del servizio con il flag Aggiorna oggetti pubblici abilitato possono caricare le attività e le librerie sul server. Tutto il contenuto della libreria delle attività e il contenuto statico vengono memorizzati come dati pubblici.

Modalità di implementazione delle attività automatiche

È possibile usare le attività automatiche per fornire assistenza agli utenti finali nell'ambiente di supporto. Le attività automatiche eseguono azioni specifiche sul computer dell'utente finale senza che l'analista o l'utente finale debbano completare il processo. Questi script consentono di acquisire informazioni telemetriche, diagnosticare i problemi dei computer e implementare risoluzioni.

Per implementare le attività automatiche, effettuare le operazioni seguenti:

1. Identificare le opportunità di automazione

   È possibile identificare i problemi comuni degli utenti finali e decidere di automatizzare alcune soluzioni per ridurre i costi dell'assistenza.

2. Ricercare l'automazione delle soluzioni

   È possibile ricercare risoluzioni a problemi comuni e raccogliere dati sui processi diagnostici che si prevede di usare.

3. Progettare attività per automatizzare il supporto fornito agli utenti finali

   È possibile progettare l'esperienza dell'utente finale che si desidera associare a ciascuna attività tramite l'editor delle attività automatiche.

4. Implementare e verificare le attività automatizzate

   È possibile verificare le attività automatiche allo scopo di stabilire se sono effettivamente in grado di risolvere i problemi comuni riscontrati nel proprio ambiente di supporto e ridurre di conseguenza i costi dell'assistenza.

5. Distribuire e monitorare le attività automatiche

   È possibile distribuire le attività automatiche agli utenti finali del proprio ambiente e permettere così agli analisti di usarle nelle sessioni di assistenza oppure allegare script ai documenti della conoscenza.

   Importante. Se ci si trova in un ambiente multi-tenancy e si desidera consentire agli analisti di caricare contenuti di attività e librerie, l'opzione Aggiornare oggetti pubblici del loro ruolo dovrà essere attiva.

Nota: CA Technologies può fornire corsi di formazione sulla creazione di attività e componenti automatici, come modelli di fasi automatiche e librerie, utilizzabili nell'ambiente. Per ulteriori informazioni sullo sviluppo di attività automatiche, rivolgersi a *CA Technologies Services*.

Amministrazione delle attività automatiche

È possibile creare attività automatiche e associarle al server. In questo caso è tuttavia necessario disporre di accesso in lettura/scrittura a tutte le tabelle correlate alle attività automatiche per poter usare l'editor delle attività automatiche. È possibile usare questa applicazione per effettuare operazioni di gestione degli utenti, come assegnare attività automatiche a ruoli e titolari.

Nota: gli analisti del fornitore del servizio che hanno accesso a più titolari possono scegliere il contesto titolare di qualsiasi operazione di aggiornamento delle attività effettuata sul server. Le attività automatiche possono anche essere impostate come pubbliche.

Distribuzione delle attività automatiche

Dopo aver creato e verificato un'attività automatica nell'editor delle attività automatiche, è possibile distribuirla a una classificazione sul server CA SDM in modo che possa essere usata per le sessioni di assistenza o self-service. Alcune delle impostazioni che non appartengono alla definizione dell'attività automatica vengono impostate al momento della distribuzione dell'attività.

È possibile caricare o scaricare le attività automatiche direttamente dal/sul server tramite l'editor delle attività automatiche. Quando si creano le classificazioni delle attività automatiche, è necessario selezionare un titolare appropriato. Se si caricano gli script sul server, è necessario selezionare la classificazione o il titolare a cui si ha accesso oppure impostare lo script come pubblico. È possibile anche importare attività automatiche dai file XSDF ed esportarli in file XSDF.

Importante Se ci si trova in un ambiente multi-tenancy e si desidera consentire agli analisti di caricare contenuti di attività e librerie, l'opzione Aggiornare oggetti pubblici del loro ruolo dovrà essere attiva.

Caricamento di un'attività automatica

È possibile caricare le attività automatiche create nell'applicazione. Quando si seleziona un'attività, vengono automaticamente caricati tutti i contenuti associati, come le librerie e il contenuto statico.

Per caricare un'attività automatica.

1. Aprire l'editor delle attività automatiche.

   Viene visualizzato l'editor delle attività Support Automation.

2. Selezionare l'attività automatica da caricare.
3. Selezionare la classificazione in cui caricare l'attività.

   Nota: se si è un utente con privilegi in un ambiente Multi-tenancy, è possibile selezionare il titolare appropriato al momento del caricamento dell'attività oppure impostare l'attività come pubblica.

4. Nella barra degli strumenti, scegliere l'icona di caricamento attività automatica.

   L'editor delle attività Support Automation carica l'attività sul server.

Modifica di un'attività automatica

È possibile scaricare attività automatiche dal server e modificarle nell'editor delle attività automatiche. Tutto il contenuto più recente rispetto a quello esistente sul server viene importato nel database e reso disponibile agli amministratori di tale titolare.

Per modificare un'attività automatica:

1. Aprire l'editor delle attività automatiche.

   Viene visualizzato l'editor delle attività Support Automation.

2. Nella barra degli strumenti, scegliere l'icona di caricamento attività automatica.

   Viene visualizzato il riquadro per l'apertura attività automatica dal server.

3. Selezionare l'attività automatica da scaricare.

   Nota: se si è un utente con privilegi in un ambiente Multi-tenancy, è possibile anche modificare le attività automatiche pubbliche o specifiche per titolare.

4. Fare clic su Apri attività.

   L'editor delle attività Support Automation scarica l'attività sul client e lo apre nell'applicazione.

   Il download crea un file di testo sul computer dell'autore dell'attività che contiene il contenuto associato.

Credenziali delle attività automatiche

Per eseguire un'attività automatica che richieda il possesso di privilegi amministrativi per l'esecuzione, come l'installazione di software, è possibile effettuare le seguenti operazioni:

- Definire credenziali predefinite per il titolare e configurare l'attività automatica in modo che utilizzi le credenziali predefinite nell'amministrazione dell'attività automatica
- Definire credenziali predefinite per il titolare e specificare che si intende utilizzare la finestra di dialogo Esegui come nella finestra Sessione di assistenza
- Definire credenziali attività automatiche per l'attività e specificare che si intende utilizzare la finestra di dialogo Esegui come nella finestra Sessione di assistenza
- Specificare le credenziali nella finestra di dialogo Esegui come nella finestra Sessione di assistenza

Assegnazione di ruoli

È possibile assegnare ruoli appropriati (come Analista, Amministratore) per consentire agli utenti di usare l'attività automatica. È possibile assegnare singole attività automatiche a ruoli specifici per consentire solo agli analisti con il ruolo assegnato di eseguire le attività automatiche. È possibile gestire i diversi set di competenze o livelli di esperienza all'interno della società di supporto.

È possibile gestire i ruoli a livello di attività selezionando alcune attività comunemente eseguite; ad esempio specificando che le attività diagnostiche devono essere automaticamente eseguite quando un utente finale accede alla sessione.

Assegnazione di un livello di accesso a un ruolo

È possibile assegnare livelli di accesso Support Automation ai ruoli CA SDM esistenti nel proprio ambiente.

Per assegnare un livello di accesso a un ruolo:

1. Selezionare Gestione ruoli e protezione, Gestione ruoli, Elenco Ruoli nella scheda Amministrazione.

   Viene visualizzata la pagina Elenco ruoli.

2. Fare clic sul ruolo a cui si desidera assegnare il livello di accesso; ad esempio Amministratore.

   Viene visualizzata la pagina Dettagli ruolo.

3. Fare clic su Modifica.

   Viene visualizzata la pagina Aggiorna ruolo.

4. Nella scheda Autorizzazione selezionare il livello di accesso creato dall'elenco a discesa Accesso SA, quindi fare clic su Salva.

   Viene visualizzata la pagina Dettagli ruolo. Verificare che l'accesso Support Automation sia stato assegnato al ruolo.

Amministrazione chat predefinita

È possibile creare risposte comuni per le domande e le situazioni più comuni. Anziché immettere più volte le stesse informazioni, è possibile salvare la risposta e usarla in altre sessioni chat.

È possibile inviare automaticamente impostazioni predefinite, come un saluto, all'inizio di ciascuna sessione. È possibile anche compilare automaticamente le impostazioni predefinite con informazioni specifiche per la sessione corrente, come il nome dell'analista.

È possibile usare i seguenti tipi di impostazioni predefinite in una sessione di assistenza:

Chat predefinita

Identifica una risposta di testo comunemente usata per una domanda di un utente finale.

URL predefinita

Identifica un URL comunemente usato a cui l'utente finale può accedere.

È possibile localizzare ciascuna impostazione predefinita della chat. L'impostazione predefinita della chat viene sincronizzata con la localizzazione dell'utente finale in modo che riceva le impostazioni predefinite localizzate corrette.

Modalità di gestione delle preimpostazioni chat

È possibile creare usare risposte predefinite per le domande e le situazioni più comuni.

1. Esaminare le sessioni di assistenza tipiche della propria organizzazione.
2. Creare preimpostazioni chat e URL che soddisfino le esigenze specifiche della propria organizzazione.
3. Specificare se le preimpostazioni devono essere impostate come specifiche per titolare o pubbliche.
4. (Opzionale) Duplicare la struttura delle preimpostazioni per gestire gli ambienti localizzati.
5. Inviare le preimpostazioni chat e URL nel corso di una sessione di assistenza.

Nota:per ulteriori informazioni su come configurare le preimpostazioni chat, consultare la *Guida in linea*.

Credenziali predefinite

È possibile eseguire operazioni automatiche sul computer dell'utente finale anche se questi normalmente non ha i diritti di accesso al sistema necessari per eseguirle. Se l'utente finale corrente non ha i diritti amministrativi necessari per la visualizzazione delle informazioni di sistema relative al proprio computer, è possibile eseguire un'operazione automatica limitata. Per ottenere accesso si utilizzeranno le credenziali predefinite.

Nota:per ulteriori informazioni su come configurare le credenziali predefinite, consultare la *Guida in linea*.

Dichiarazioni di non responsabilità

Quando lanciano attività self-service, gli utenti visualizzano una dichiarazione di non responsabilità. Devono dare il loro accordo per poter continuare.

È possibile creare, aggiornare ed eliminare gli oggetti di business della dichiarazione di non responsabilità.

Nota:per ulteriori informazioni su come configurare le dichiarazioni di responsabilità Support Automation, consultare la *Guida in linea*.

Amministrazione del registro sessione

Il registro sessione consente di visualizzare tutte le azioni eseguite dall'analista durante la sessione di assistenza, come gli strumenti usati e i dettagli della chat (eccetto i messaggi privati). È possibile stampare il registro sessione o inviarlo per posta elettronica all'utente finale. Gli utenti finali possono anche visualizzare e salvare il registro, ma non modificarlo.

Visualizzazione del registro sessione

Il registro sessione viene aggiornato con tutte le azioni eseguite durante la sessione di assistenza, come le sessioni in modalità chat (escluse le conversazioni private), i risultati delle attività automatiche e l'uso di uno strumento specifico dell'interfaccia Analista Support Automation.

Per visualizzare il registro sessione:

1. Aprire la visualizzazione della sessione attiva.

   Viene visualizzata la pagina Sessione attiva.

2. Selezionare il registro sessione dalla barra degli strumenti del menu Sessioni.

   Viene visualizzata la pagina Registro sessione.

3. Fare clic su Aggiorna.

   La pagina si aggiorna.

4. (Opzionale) Selezionare la casella di controllo per l'aggiornamento automatico.
5. (Opzionale) Fare clic su Salva registro sul disco.

   Viene visualizzata la finestra di dialogo Salva. È possibile salvare il registro sessione localmente come file HTML.

Report Support Automation

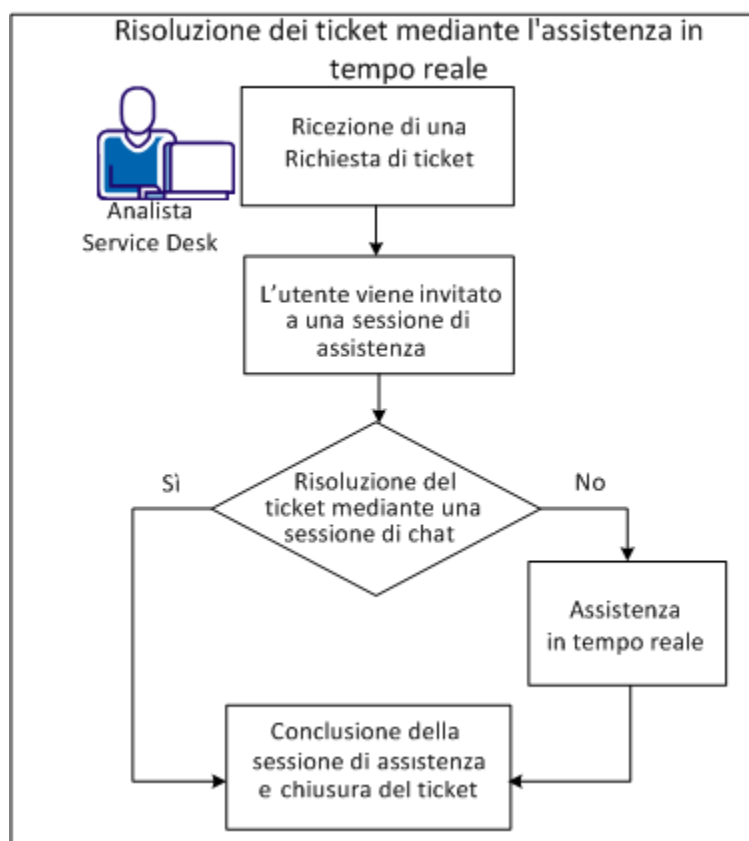
CA Business Intelligence installa un set di report Support Automation predefiniti. CA SDM distribuisce automaticamente questi report al server BusinessObjects al momento dell'installazione.

I ruoli Amministratore Support Automation e Analista Support Automation possono utilizzare BusinessObjects InfoView per visualizzare informazioni dettagliate e di riepilogo sui seguenti elementi:

- Metriche di accesso dell'analista
- Metriche delle sessioni di assistenza
- Metriche delle voci delle code
- Metriche dell'esecuzione delle attività automatiche
- Utilizzo dello strumento per categoria di ticket
- Dati in tempo reale relativi agli utenti finali inseriti nelle code di supporto, alle sessioni di assistenza attive e agli analisti attivi (connessi).

Nota: per ulteriori informazioni sull'uso di BusinessObjects InfoView, vedere le informazioni su CA Business Intelligence nella *Guida in linea*.
Risoluzione dei ticket mediante l'assistenza in tempo reale

Durante una *sessione di assistenza* gli analisti di Service Desk forniscono assistenza in tempo reale agli utenti finali per la risoluzione dei ticket in CA SDM. È visualizzare le informazioni relative a un problema informatico di un utente finale nel ticket di CA SDM. Inoltre, è possibile comunicare via chat con l'utente e invitarlo a una sessione di assistenza. Utilizzare la funzionalità Support Automation di CA SDM per risolvere ticket con assistenza in tempo reale. Ad esempio, l'utente finale crea un ticket per un problema di connessione di rete con un'applicazione software.

Il diagramma seguente descrive la risoluzione di un ticket da parte di un analista di Service Desk mediante l'assistenza in tempo reale:

Eseguire le operazioni seguenti per fornire l'assistenza in tempo reale e risolvere un ticket CA SDM:

1. Ricezione di una richiesta di ticket (a pagina 1100).
2. L'utente viene invitato a una sessione di assistenza (a pagina 1100).
3. Risoluzione del ticket mediante una sessione di chat (a pagina 1101) o l'assistenza in tempo reale (a pagina 1101).
4. Conclusione della sessione di assistenza e chiusura del ticket (a pagina 1102).

Ricezione di una Richiesta di ticket

Un utente inoltra un ticket con la descrizione del problema rilevato sul computer in uso. Visualizzare i dettagli del ticket in un avviso di posta elettronica oppure nel contatore di CA SDM. Ad esempio, l'utente non può utilizzare un'applicazione software configurata per la sincronizzazione con la rete.

Procedere come descritto di seguito:

1. Accedere a CA SDM e selezionare Contatore, Coda personale.
2. Aprire un ticket.
3. Consultare la descrizione del ticket.
4. (Facoltativo) Aggiungere un commento al ticket per richiedere ulteriori informazioni all'utente riguardo l'applicazione software.

Invito dell'utente a una sessione di assistenza

Invitare l'utente a una sessione di assistenza per risolvere il ticket. Ad esempio, richiedere informazioni sulle impostazioni di rete del computer dell'utente finale.

Procedere come descritto di seguito:

1. Nella scheda Support Automation della pagina Dettagli del ticket, fare clic su Invita utente finale.
2. Inviare un messaggio di benvenuto all'utente finale.
3. Fare clic su Avvia.

   L'Interfaccia Analista di Support Automation viene visualizzata. Attendere che l'utente si unisca alla sessione di assistenza.

Risoluzione del ticket mediante una sessione di chat

Iniziare una sessione di chat. L'utente riceve una notifica di posta elettronica da CA SDM. Questo messaggio di posta elettronica contiene un collegamento alla sessione di assistenza e ai dettagli del ticket. Il collegamento apre il client dell'utente finale di Support Automation sul computer dell'utente. Consultare l'utente per decidere come risolvere il ticket.

Nota: se l'utente finale non può partecipare alla sessione di assistenza utilizzando l'URL, inviare un messaggio di posta elettronica per richiedere all'utente di selezionare il collegamento Contatta analista della pagina iniziale di Self-service.

Procedere come descritto di seguito:

1. Fare clic sulla scheda Chat dell'interfaccia Analista di Support Automation.
2. Eseguire una delle seguenti operazioni:
   - Selezionare una domanda, un'istruzione o un URL dall'elenco a discesa Impostazioni predefinite di chat.
   - Immettere il testo desiderato nella finestra della chat e fare clic su Invio.

     Ad esempio, chiedere all'utente finale informazioni sulle porte di rete specificate durante la configurazione dell'applicazione software.
   - Inserire un URL specifico per l'utente finale.

     L'utente finale apre manualmente il collegamento nel browser in uso.

Assistenza in tempo reale

Utilizzare l'interfaccia Analista di Support Automation per fornire l'assistenza in tempo reale eseguendo le operazioni necessarie sul computer dell'utente finale. Ad esempio, eseguire lo script di diagnostica, esplorare il file system e monitorare il computer dell'utente finale in remoto. Ad esempio, durante la chat con l'utente viene stabilito che è possibile risolvere il problema di sincronizzazione dell'applicazione software mediante una sessione di assistenza in tempo reale.

Procedere come descritto di seguito:

1. Nell'interfaccia Analista di Support Automation, selezionare la scheda dello strumento appropriato per la risoluzione del ticket:
   - Attività automatiche: selezionare un'attività automatica dal riquadro di sinistra e fare clic su Esegui. Ad esempio, eseguire uno script per la configurazione delle impostazioni di rete per l'applicazione software.
   - Esplora file: esplorare il file system dell'utente. Ad esempio, esplorare il disco rigido per individuare un file specifico nella directory di installazione dell'applicazione software.

- Trasferimento file: trasferire un file da un computer all'altro. Ad esempio, trasferire un file dal proprio computer per sostituire un file danneggiato nella directory di installazione.
- Registro remoto: esplorare il registro di sistema dell'utente finale e modificare le voci di registro. Ad esempio, modificare i valori del registro di sistema per l'applicazione software.
- Strumenti sistema remoto: eseguire un programma sul computer dell'utente finale o forzare il riavvio. Ad esempio, eseguire l'interfaccia di configurazione dell'applicazione software.
- Controllo remoto: controllare il computer dell'utente finale in remoto. Ad esempio, controllare il computer dell'utente finale per configurare l'applicazione software.
- Cattura di schermata: eseguire una cattura di schermata del computer dell'utente finale. Ad esempio, nel caso in cui i problemi di connessione non consentano il controllo remoto del computer l'analista può guidare l'utente basandosi sulle catture di schermata.

2. Selezionare Controllo remoto e configurare l'applicazione software da sincronizzare con la rete aziendale.
3. Verificare con l'utente che l'applicazione software esegua correttamente la sincronizzazione e risolvere il ticket.

Conclusione della sessione di assistenza e chiusura del ticket

Dopo avere verificato che il ticket è stato risolto, aggiornare il ticket e chiudere la sessione di assistenza.

Procedere come descritto di seguito:

1. Fare clic su Finire nell'interfaccia Analista di Support Automation per chiudere la sessione.

   L'utente riceve una notifica di posta elettronica con il registro di sessione.
2. (Facoltativo) Fare clic su Registro di sessione per visualizzare i registri della chat e i risultati dello strumento Support Automation.
3. Fare clic sul numero di ticket nell'interfaccia Analista di Support Automation. Ad esempio, fare clic su Incidente 40.

   Viene visualizzata la pagina dei dettagli dell'Incidente 40 in CA SDM.
4. Fare clic su Modifica.

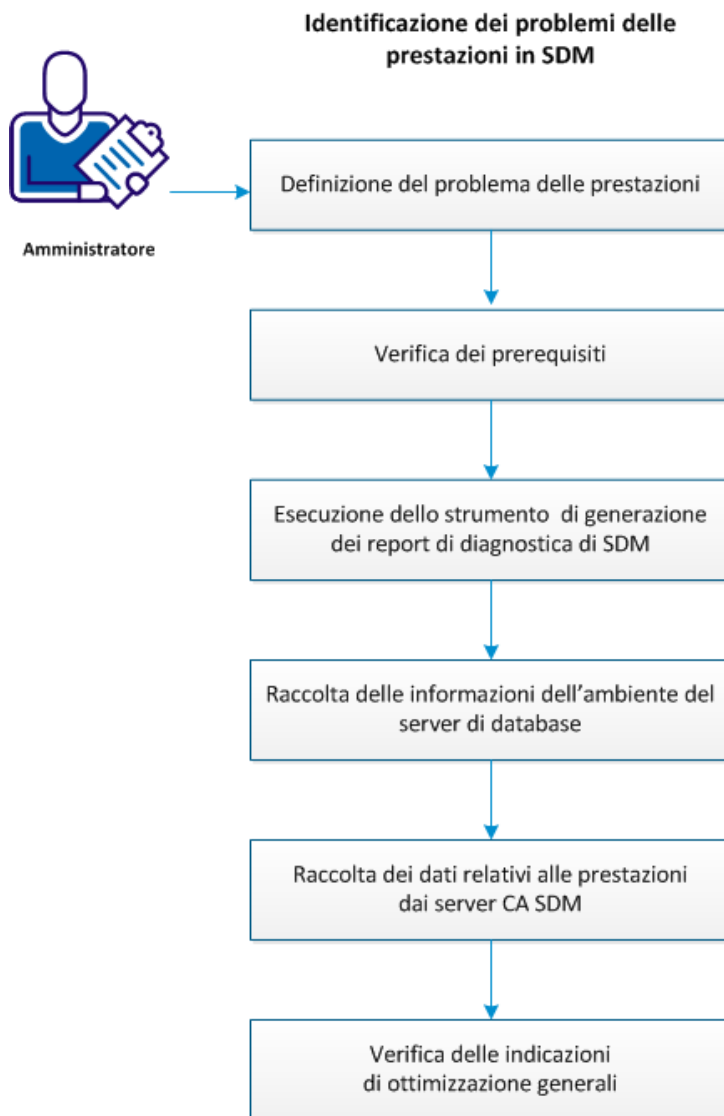
5. Modificare lo stato del ticket in SA-Risolto.
6. Fare clic su Salva e chiudi.

   Il registro attività del ticket viene salvato e il processo di assistenza in tempo reale viene completato.

Capitolo 25: Identificazione dei problemi di prestazioni in CA SDM

In qualità di amministratori di sistema, è possibile raccogliere le informazioni riguardanti ambiente di installazione, uso delle risorse, dettagli di configurazione e altre risorse di sistema disponibili. Ad esempio, consultare la configurazione del computer per individuare il tipo di sistema operativo, la versione e le risorse di sistema disponibili. Questi dati consentono di identificare e a diagnosticare un problema di prestazioni o relativo alla memoria in CA SDM. Lo strumento di report diagnostico di CA e l'utilità di registrazione periodica permettono di raccogliere le informazioni diagnostiche sull'ambiente di CA SDM in uso.

Il diagramma seguente descrive la procedura per raccogliere informazioni diagnostiche e identificare i problemi di prestazioni in CA SDM:

Equation 2: Identificazione dei problemi relativi alle prestazioni nei server di CA SDM

Attenersi alla procedura seguente:

1. Definizione del problema di prestazioni (a pagina 1107).
2. Verifica dei prerequisiti
3. Esecuzione dello strumento di report diagnostico di CA SDM (a pagina 1109).
   - Verifica del report di Windows
   - Verifica del report di UNIX
   - Verifica del report diagnostico dei dati raccolti
4. Raccolta dei dettagli di ambiente del server di database (a pagina 1114).
5. Raccolta dei dati sulle prestazioni dai server di CA SDM
6. Verifica delle indicazioni di ottimizzazione (a pagina 1119).

Definizione i problemi di prestazioni

È possibile definire i problemi di prestazioni rilevati durante la raccolta delle informazioni di sistema. Consultare l'elenco seguente delle domande di esempio per determinare se sono pertinenti al problema riscontrato:

- Quali sono i sintomi rilevati dagli utenti che interrompono le attività?
- Quando è stato rilevato il problema per la prima volta?
- L'ambiente in uso è stato modificato recentemente, ad esempio sono stati eseguiti aggiornamenti dell'hardware?
- Quale funzionalità del prodotto presenta il problema?
- Quanti utenti hanno rilevato il problema? Quale tipo di utente è interessato?
- Quali utenti non hanno riscontrato alcun impatto?
- Qual è la posizione geografica degli utenti che hanno riscontrato il problema?
- Di quale livello di accesso dispongono gli utenti interessati?
- CA SDM è ospitato su un server VMWare ESX o un altro ambiente virtualizzato?
- Quale altro software è in esecuzione sul server ESX o sul computer host?
- Quali sono le specifiche di ambiente?
- Quante CPU sono presenti su ciascun computer?
- Quanta memoria è stata configurata per ciascun computer?

Verifica dei prerequisiti

1. Per sistema operativo Windows, installare lo strumento pslist.exe e aggiungere la variabile di percorso della directory su ciascun server di CA SDM.
2. Installare e configurare i server di CA SDM prima di eseguire lo strumento di diagnostica.

   Nota: si consiglia di contattare il supporto in linea di CA prima di utilizzare lo strumento di diagnostica.

Installazione degli strumenti Ps per Windows

Per un'installazione di Windows, installare lo strumento pslist.exe e aggiungere la variabile di percorso della directory alla variabile di percorso di sistema.

Attenersi alla procedura seguente:

1. Scaricare PS Tool Suite da Microsoft.
2. Estrarre pstools.zip in una directory selezionata e aggiungere la directory alla variabile di ambiente %PATH% di Windows.
3. Eseguire pslist.exe una volta manualmente dal prompt dei comandi come utente di sistema locale e accettare il contratto di licenza. Per eseguire pslist.exe come utente di sistema locale, immettere il comando seguente:

   ```
   psexec.exe -s -i pslist.exe
   ```

   Nota: È possibile avviare il servizio di Windows di CA SDM con un account utente diverso da quello del sistema locale. Per tale servizio, eseguire pslist.exe con l'account diverso e accettare il contratto di licenza. Se pslist.exe viene aggiunto dopo l'installazione e la configurazione di CA SDM, riavviare i servizi di CA SDM una volta accettato il contratto di licenza di pslist.

Raccolta delle informazioni dallo strumento di report diagnostico CA

Il supporto di installazione di CA SDM include lo strumento di report diagnostico che permette di raccogliere informazioni per diagnosticare problemi relativi alle prestazioni. È possibile utilizzare lo strumento di diagnostica per raccogliere informazioni sul tipo di sistema operativo e decidere quali comandi utilizzare per la raccolta dei dati dall'installazione di CA SDM.

Configurare il server di CA SDM prima di eseguire lo strumento di diagnostica.

Attenersi alla procedura seguente:

Windows

1. Impostare $NX_ROOT come la directory principale dell'installazione di CA SDM.

   La posizione predefinita per $NX_ROOT è C:\Programmi\CA\Service Desk\. È possibile modificare i valori predefiniti durante la modifica della directory predefinita durante il processo di installazione.

2. Verificare che la variabile del percorso di sistema includa $NX_ROOT\bin.

UNIX/Linux

1. Impostare $NX_ROOT come la directory principale dell'installazione di CA SDM.

   Il valore predefinito di $NX_ROOT sui sistemi operativi Unix o Linux è —/opt/CAisd/. È possibile modificare i valori predefiniti durante la modifica della directory predefinita durante il processo di installazione.

2. Verificare che la variabile $PATH includa $NX_ROOT/bin.

Esecuzione dello strumento di report diagnostico

Lo strumento di diagnostica di CA crea un file .caz sul sistema operativo Windows e un file .tar.gz su UNIX nella directory $NX_ROOT\diag\rpt caricata insieme al problema sul sito http://support.ca.com.

Attenersi alla procedura seguente:

1. Eseguire supp_diag.cmd su Windows, o supp_diag.sh su UNIX.

   Lo strumento di diagnostica può richiedere da cinque a dieci minuti per completare l'operazione.

2. Se il processo di raccolta dei dati non viene completato, visualizzare i file di registro $NX_ROOT\diag\<host_name>_supp_diag.log per individuare gli errori che si sono verificati durante la raccolta delle informazioni di diagnostica.

   Nota: premere CTRL+C se si desidera annullare il processo batch in background. L'esecuzione in background di alcuni processi, ad esempio MSINFO32.exe, non viene interrotta. Per qualsiasi dubbio sull'utilizzo dello strumento di diagnostica, contattare il supporto in linea di CA.

3. La struttura della directory di script mostra la posizione dei file di script, dei file zip di diagnostica e dei file di registro:

   - La directory $NX_ROOT\diag\bin contiene i file script.
   - La directory $NX_ROOT\diag\rpt contiene il file .zip di diagnostica (in formato .caz per Windows e .tar.gz per i sistemi UNIX).
   - La directory $NX_ROOT\diag\misc_logs contiene i file di registro che è possibile includere automaticamente nel file .zip.

4. Completare le operazioni necessarie per decomprimere i file raccolti in base al sistema operativo:

   Windows

   - Aprire un prompt dei comandi.
   - Utilizzare il comando cd per accedere a $NX_ROOT\diag\rpt o alla directory del file .CAZ.
   - Eseguire il seguente comando:

     ```
     $NX_ROOT\diag\bin\cazipxp -u <package_name>.CAZ
     ```

   UNIX

   - Aprire un prompt dei comandi.
   - Utilizzare il comando cd per accedere a $NX_ROOT/diag/rpt o alla directory del file .tar o .tar.gz
   - Decomprimere il file:

     ```
     gunzip -d <package_name>.tar.gz
     tar -xvf <package_name>.tar
     ```

Verifica del report di Windows

L'elenco seguente descrive i file di report di Windows creati e inclusi nel pacchetto di file CAZ\tar.

Ca.olf

Specifica le informazioni sulla licenza CA dalla directory ca_lic.

Lic98.log

Specifica il file di registro associato alla licenza CA dalla directory ca_lic.

Lic98version.log

Specifica il file di registro associato alla licenza CA dalla directory ca_lic.

Licdebug.log log

Specifica il file associato alla licenza CA dalla directory ca_lic.

Drwatsoninfo.txt

Specifica la configurazione del programma Dr Watson del computer.

<nome host>_env.txt

Specifica le variabili di ambiente impostate sul computer.

<nome host>_slstat.txt

Specifica l'output del comando slstat.

<nome host>_pdm_status.txt

Specifica l'output del comando slstat.

<nome host>_dir_listing.txt

Specifica l'elenco delle directory di installazione di CA Service Desk

<nome host>_pslist.txt

Specifica l'elenco dei processi dopo l'installazione dello strumento PSList di Microsoft.

<nome host>_MSINFO32.NFO

Specifica le informazioni di sistema di raccolta di output MSINFO

<nome host>_SYSTEMINFO.TXT

Specifica le informazioni di sistema.

<nome host>_appevents.csv

Specifica i registri eventi dell'applicazione creati nei sette giorni precedenti.

<nome host>_sysevents.csv

Specifica i registri eventi dell'applicazione creati nei sette giorni precedenti.

<nome host>_hostinfo.txt

Specifica le informazioni del computer.

<nome host>_prodinstallinfo.txt

Specifica le informazioni di installazione dei prodotti CA.

<nome host>_caprod_registry.txt

Specifica le informazioni del Registro di Sistema dei prodotti CA installati.

<nome host>_softfeatures.txt

Specifica l'elenco delle funzionalità software installate per Service desk.

<nome host>_ipconfig.txt

Specifica le informazioni relative al file di configurazione IP.

<nome host>_supp_diag.log

Specifica il registro creato per l'esecuzione dello strumento supp_diag.

Verifica del report di UNIX

L'elenco seguente descrive i file di report di UNIX creati e inclusi nel pacchetto di file CAZ\tar.

Ca.olf

Specifica le informazioni sulla licenza CA dalla directory ca_lic.

Lic98.log

Specifica il file di registro associato alla licenza CA dalla directory ca_lic.

<nome host>_env.txt

Specifica le variabili di ambiente impostate sul computer.

<nome host>_slstat.txt

Specifica l'output del comando slstat.

<nome host>_pdm_status.txt

Specifica l'output del comando slstat.

<nome host>_dir_listing.txt

Specifica l'elenco delle directory di installazione di CA Service Desk

<nome host>_pslist.txt

Specifica l'elenco dei processi dopo l'installazione dello strumento PSList di Microsoft.

<nome host>_uname.txt

Specifica l'output del comando di sistema operativo uname.

<nome host>_diskinfo.txt

Specifica l'output del comando di sistema operativo df.

<nome host>_freemem.txt

Specifica l'output delle informazioni di memoria.

<nome host>_supp_diag.log

Specifica il registro creato per l'esecuzione dello strumento supp_diag.

<nome host>_prtconf.txt

Specifica l'output del comando di sistema operativo prtconf su Solaris e sui computer AIX.

<nome host>_solrev.txt

Specifica la versione di sistema operativo e le informazioni relative alle patch sui computer Solaris.

<nome host>_netconf.txt

Specifica le informazioni di configurazione IP sui computer AIX.

Verifica del report diagnostico dei dati raccolti

L'elenco predefinito dei file\directory della documentazione CA SDM include i seguenti report nel file CAZ\tar. Aggiungere i file o le directory inclusi nel file CAZ\tar inserendoli nella directory $NX_ROOT\diag\misc_logs.

- $NX_ROOT/GENLEVEL or$NX_ROOT/.GENLEVEL
- $NX_ROOT/<COMPUTERNAME>.his
- $NX_ROOT/NX.env
- $NX_ROOT/NX.env.last
- $NX_ROOT/log\
- $NX_ROOT/pdmconf\
- $NX_ROOT/pdmconf\version
- $NX_ROOT/bopcfg\www*.cfg
- $NX_ROOT/site\mods\

- $NX_ROOT/site\ddict.sch
- $NX_ROOT/site\eh\
- $NX_ROOT/bopcfg\www\CATALINA_BASE\logs\
- $NX_ROOT/bopcfg\www\CATALINA_BASE\webapps\CAisd\WEB-INF\web.xml
- $NX_ROOT/bopcfg\www\CATALINA_BASE\webapps*.xml

Raccolta dei dettagli di ambiente del server di database

È possibile raccogliere le informazioni sul server di database per identificare i problemi legati alle prestazioni in CA SDM.

Procedere come descritto di seguito:

1. Individuare la posizione del server di database, ad esempio locale o remoto.
2. Individuare la versione di DBMS, la versione del sistema operativo e il livello di patch.
3. Completare le operazioni appropriate per il tipo di database:
   - Eseguire le query seguenti per SQL Server e annotare i risultati:

     ```
     select @@version
     SELECT SERVERPROPERTY('productversion'), SERVERPROPERTY ('productlevel')
     ```

   - Eseguire la seguente query per Oracle:

     ```
     select * from v$version where banner like 'Oracle%';
     ```

4. Confermare la versione del client di database installato sul server applicazioni.
5. Se disponibile, raccogliere le informazioni sui dati di ambiente, ad esempio il sistema operativo e altri database.
6. Raccolta della topologia di rete e delle informazioni di topologia o di altri prodotti integrati con CA SDM.

   Ad esempio, individuare le informazioni sui prodotti nei file PDF o diagrammi disponibili.

Raccolta dei dati sulle prestazioni dai server di CA SDM

È possibile raccogliere i dati relativi all'utilizzo delle risorse sui server di CA SDM differenti in una configurazione multi-server per determinare i problemi riscontrati su ciascun server. I set di dati raccolti vengono utilizzati per analizzare e risolvere i problemi legati alle prestazioni o relativi alla memoria nei server di CA SDM. L'utilità di registrazione periodica consente di avviare o arrestare la raccolta dei dati di diagnostica mediante l'interfaccia Web di CA SDM. È possibile condividere il set di dati raccolti con il supporto in linea di CA per identificare e risolvere i problemi dei server di CA SDM.

L'utilità di registrazione periodica viene eseguita sul daemon pdm_intrvlog_nxd che raccoglie i dati di registro da un server. Il daemon si avvia automaticamente all'avvio di un server di Service Desk.

- Per interrompere il daemon di registrazione periodica manualmente, rimuovere la voce dell'utilità di registrazione periodica da pdm_startup
- Per avviare il daemon di registrazione periodica manualmente, fare doppio clic sul file pdm_intrvlog_nxd.bat nella cartella $NX_ROOT/bin

Raccolta dei dati sull'utilizzo mediante la registrazione periodica

Per raccogliere i dati relativi all'utilizzo delle risorse sui server di CA SDM, configurare il server per la registrazione periodica. È possibile selezionare il tipo di dati che si desidera raccogliere da ciascun server e modificare le opzioni di registrazione dei server in qualsiasi momento.

Ad esempio, se si seleziona solo l'opzione relativa all'utilizzo della CPU per un server specifico, l'utilità raccoglie solo i dati per l'utilizzo della CPU sul server.

Attenersi alla procedura seguente:

1. Accedere a CA SDM.
2. Nella scheda Amministrazione, selezionare Sistemi, Registrazione periodica.

   Viene visualizzato l'elenco delle configurazioni della registrazione periodica.
3. Fare clic su Crea Nuovo per aggiungere una configurazione del registro periodico.

   Viene visualizzata la pagina Crea nuova configurazione del registro periodico.
4. Inserire i dati nei seguenti campi:

   Nome server

   Specifica il server per cui si desidera eseguire la raccolta dei dati di registro. Utilizzare l'icona Cerca per visualizzare l'elenco dei server configurabili per la registrazione periodica.

   Intervallo di ricorrenza

   Specifica l'intervallo di tempo durante cui i dati di registro vengono raccolti per il server. Ad esempio, se l'intervallo di ricorrenza viene impostato su 3 minuti, il registro viene raccolto ogni 3 minuti.

   Valore predefinito: 3 minuti

   Valore minimo: 2 minuti

   Abilitato

   Indica se la registrazione periodica è abilitata o disabilitata per il server. Se abilitata, il registro periodico viene raccolto per il server.

   Nota: Per interrompere la registrazione periodica prima della data di fine pianificata, modificare lo stato Abilitato in NO.

   Stato record

   Indica se la configurazione del registro periodico è attiva o non attiva.

   Data di inizio pianificata

   Specifica la data e l'ora di inizio dell'operazione di raccolta dei dati di registro. Se non si immette una data di inizio, la registrazione periodica si avvia immediatamente finché la configurazione è attiva e abilitata o fino alla data di fine pianificata.

Data di fine pianificata

Specifica la data e l'ora di fine dell'operazione di raccolta dei dati di registro. Se non si immette una data di fine, l'esecuzione della registrazione periodica continuerà finché la configurazione è attiva e abilitata.

5. Selezionare l'opzione di registro appropriata per la raccolta dati dal server.

   Ad esempio, selezionare Utilizzo CPU se si desidera acquisire il registro dei dati relativi all'utilizzo della CPU.

Utilizzo CPU

Consente di raccoglie i dati statistici circa l'utilizzo della CPU per il server tramite l'esecuzione di pslist -x su Windows o di "ps" su Unix. A seconda del tipo di configurazione, è possibile raccogliere i dati di diagnostica sui server seguenti:

- Convenzionale: server primario.
- Disponibilità avanzata: tutti i server.

Utilizzo memoria

Consente di raccogliere i dati circa l'utilizzo della memoria per il server tramite l'esecuzione di pslist -m su Windows o di "ps" su Unix. A seconda del tipo di configurazione, è possibile raccogliere i dati di diagnostica sui server seguenti:

- Convenzionale: server primario.
- Disponibilità avanzata: tutti i server.

Stato rete

Consente di raccogliere le informazioni di tutte le connessioni attive e le statistiche di rete tramite l'esecuzione di netstat /b o /a dal sistema operativo. A seconda del tipo di configurazione, è possibile raccogliere i dati di diagnostica sui server seguenti:

- Convenzionale: server primario.
- Disponibilità avanzata: tutti i server.

Elenco Attività

Consente di raccogliere le informazioni sull'applicazione e sui servizi per tutte le attività in esecuzione sul server. A seconda del tipo di configurazione, è possibile raccogliere i dati di diagnostica sui server seguenti:

- Convenzionale: server primario.
- Disponibilità avanzata: tutti i server.

Numero sessioni Web

Consente di raccogliere le sessioni di CA SDM e le statistiche utente per i processi del motore Web tramite l'esecuzione del comando pdm_webstat. È possibile raccogliere i dati per qualsiasi server di CA SDM.

Stato server

Consente di raccogliere le informazioni su tutti i daemon o i processi di CA SDM sul server tramite l'esecuzione del comando pdm_status. È possibile raccogliere i dati per qualsiasi server di CA SDM.

Report database

Consente di raccogliere le informazioni sui tipi di record del database tramite l'esecuzione del comando db_report. È possibile raccogliere i dati per qualsiasi server di CA SDM.

Informazioni database virtuale

Consente di raccogliere le informazioni relative alle richieste di database in coda tramite l'esecuzione del comando pdm_vdbinfo. È possibile raccogliere i dati per qualsiasi server di CA SDM.

Elenco connessioni server

Consente di raccogliere le informazioni sulle connessioni attive per il server tramite l'esecuzione del comando pdm_listconn. È possibile raccogliere i dati per qualsiasi server di CA SDM.

Elenco processi slump

Consente di raccogliere le informazioni su processi e connessioni slump tramite l'esecuzione del comando slstat. È possibile raccogliere i dati per qualsiasi server di CA SDM.

6. Fare clic su Salva.

   Il server è stato configurato per la registrazione periodica.

7. (Facoltativo) Ripetere i passaggi 1-5 per creare altre configurazioni del registro periodico.

8. Accedere alla directory $NX_ROOT\log e visualizzare i file di registro generati. A seconda delle opzioni selezionate per la registrazione periodica, vengono generati i file di output seguenti:

   - cpu_usage_hostname
   - db_report_hostname
   - memory_usage_hostname
   - netstat_hostname
   - pdm_listconn_hostname
   - pdm_vdbinfo_hostname
   - server_status_hostname
   - session_counts_hostname
   - tasklist_hostname

Importante. Il limite massimo predefinito per le dimensioni del file di output è 30 KB. È possibile modificare le dimensioni del file cambiando il valore @NX_LOGFILE_LIMIT nel file NX_env. Se i file di output generati superano il limite massimo per le dimensioni del file, viene creato un nuovo file con il suffisso 1. I file generati successivamente contengono il suffisso con il numero in modo incrementale.

È possibile condividere i dati di registro raccolti con il supporto tecnico di CA per identificare i problemi relativi alle prestazioni dell'installazione in uso di SDM.

Verifica delle indicazioni di ottimizzazione

Come procedura ottimale si consiglia di controllare regolarmente gli indicatori chiave delle prestazioni e l'utilizzo delle risorse. Verificare inoltre l'esecuzione della manutenzione regolare per individuare più facilmente eventuali problemi e risolverli in modo tempestivo.

Se si rileva la presenza di un problema, o se gli utenti riportano un rallentamento delle prestazioni, riportare il problema al supporto in linea di CA inviando i dati della registrazione periodica, il report dello strumento di diagnostica di CA SDM, i registri standard di CA SDM e le informazioni relative al problema. Inviare le informazioni al supporto tecnico CA da ciascun server di CA SDM.

L'elenco seguente riporta i sintomi comuni in caso di problemi di prestazioni:

- Messaggi lunghi nei registri standard di CA SDM (file stdlog.x)
- Cercare nei registri stdlogs i messaggi il cui testo inizia con "The following query took #### milliseconds...".
- Accodamento degli agenti di database nell'output di pdm_vdbinfo
- Cercare le richieste in coda (*Queued Requests(#)*nell'output di pdm_vdbinfo. È possibile eseguire manualmente questo comando al prompt del sistema operativo. Questo comando viene eseguito anche dallo script per la registrazione periodica.
- Numero elevato di utenti connessi a ciascun motore Web. Ad esempio, più di 200 utenti.

  Nota: eseguire pdm_webstat per visualizzare il numero di utenti simultanei per il motore Web. È possibile eseguire manualmente questo comando al prompt del sistema operativo. Questo comando viene eseguito anche dallo script per la registrazione periodica.
- Reclami dell'utente

Appendice A: Comandi di riferimento

Questa appendice fornisce una descrizione dettagliata dei comandi di riferimento disponibili per CA SDM.

Questa sezione contiene i seguenti argomenti:

bop_sinfo--Visualizzazione delle informazioni di sistema (a pagina 1122)
dbmonitor_nxd--Daemon monitoraggio database (a pagina 1123)
pdm_backup - Scrittura di tabelle di database in file ASCII (a pagina 1124)
pdm_cache_refresh - Aggiornamento del database (a pagina 1126)
pdm_configure - Apertura della finestra di configurazione (a pagina 1127)
pdm_d_refresh - Avvio dei daemon con errori (a pagina 1128)
pdm_deref - Annullamento del riferimento (dati in formato ASCII) (a pagina 1128)
pdm_discimp - Importazione degli asset rilevati (a pagina 1132)
pdm_discupd -- Aggiornamento asset rilevati (a pagina 1134)
pdm_extract - Estrazione dei dati dal database (a pagina 1134)
pdm_halt - Arresto dei daemon o dei servizi (a pagina 1138)
pdm_init - Avvio dei daemon (a pagina 1138)
pdm_key_refresh - Aggiornamento delle informazioni chiave nella cache (a pagina 1139)
pdm_lexutil--Modifica del dizionario di CA SDM (a pagina 1139)
pdm_k_reindex—Utilità di reindicizzazione della conoscenza (a pagina 1140)
pdm_listconn - Elenco delle connessioni attive (a pagina 1144)
pdm_load - Aggiunta, aggiornamento ed eliminazione dei record del database (a pagina 1146)
pdm_logfile - Modifica delle dimensioni cutover del file stdlog (a pagina 1148)
Utilità pdm_log4j_config - Modifica del file delle proprietà log4j (a pagina 1149)
pdm_proctor_init - Avvio di proctor sui server secondari (a pagina 1154)
pdm_replace - Sostituzione di una tabella di database (a pagina 1154)
Gestione dell'applicazione dei servizi Web RESTful di CA SDM - pdm_rest_util (a pagina 1156)
pdm_restore - Ripristino di un database (a pagina 1157)
pdm_status - Stato dei daemon e dei processi (a pagina 1159)
pdm_task - Impostazione delle variabili di ambiente (a pagina 1159)
Interfaccia riga di comando di Text API - pdm_text_cmd (a pagina 1160)
pdm_uconv - Conversione di set di caratteri in UTF-8 (a pagina 1163)
pdm_userload - Aggiunta, aggiornamento ed eliminazione dei record del database (a pagina 1166)
pdm_webstat - Statistiche sull'uso del Web (a pagina 1169)
report - Generazione dei rapporti (a pagina 1173)
rpt_srv - Generazione dei rapporti (a pagina 1174)
uniconv - Avvio del daemon convertitore eventi CA NSM UNIX (a pagina 1175)
Utilità pdm_mail - Invio di informazioni di posta elettronica (a pagina 1176)
Utilità pdm_server_control--Identificazione dei server (a pagina 1179)

bop_sinfo--Visualizzazione delle informazioni di sistema

L'utilità bop_sinfo visualizza le informazioni relative a un oggetto singolo definito Majic. È possibile eseguire questa utilità sugli oggetti elencati nella *Guida di riferimento tecnico*.

Sintassi

Il comando presenta il seguente formato:

```
bop_sinfo [-s server] [-p] [-l] [-d] [f] [-q] [-t] [-m] [-a] object [-h]
```

-s server

Specifica il server per la query.

-p

Visualizza le informazioni del produttore.

-l

Visualizza l'elenco domset.

-d

Visualizza informazioni di oggetto di database, incluso il nome e il tipo di tutti gli attributi.

-f

Visualizza informazioni sulla factory, inclusi rel_attr e common_name.

-q

Visualizza il nome dello schema della tabella associata.

-t

Visualizza i trigger nell'oggetto.

-m

Visualizza i metodi usati dall'oggetto.

-a

Visualizza i dettagli di attributo.

object

Nome dell'oggetto di cui eseguire la query

-h

Visualizza la Guida in linea dell'utilità.

Esempio: visualizzazione delle informazioni di sistema per l'oggetto dmn

```
bop_sinfo -d dmn

Factory dmn
 Attributi
    id                  INTEGER
    producer_id LOCAL STRING(20)
    persistent_id       STRING(30)
    sym                 STRING(60) REQUIRED
    delete_flag SREL -> actbool.enum REQUIRED
    desc        STRING(40)
    tables              BREL <- dcon.dom_id {dom_id = ?}
    last_mod            DATE
    last_mod_by SREL -> cnt.id
    audit_useridLOCAL SREL -> cnt.id
```

dbmonitor_nxd--Daemon monitoraggio database

Il daemon monitoraggio database (dbmonitor_nxd) fornisce un meccanismo che consente l'aggiornamento della cache CA SDM di tabelle di database specifiche quando vengono eseguite modifiche esternamente da CA SDM.

La funzione principale di dbmonitor_nxd consiste nel creare notifiche CHANGE per modifiche in tabelle specifiche che non si verificavano attraverso CA SDM. Per eseguire questa funzione, il monitor effettua query periodiche al database, determina quali siano le modifiche esterne e quindi invia notifiche CHANGE al server bpvirtdb_nxd. Il server bpvirtdb_nxd notifica la modifica a tutti i server domsrvr, e ciò comporta l'aggiornamento della cache di ciascun domsrvr per oggetti di database specifici e quindi notifica tutti gli altri processi che sottoscrivono modifiche nelle tabelle specifiche.

Questo meccanismo funziona bene per la modifica esterna occasionale nelle tabelle monitorate. Tuttavia, nei casi in cui vengono effettuati esternamente aggiornamenti di massa, viene trasmessa una serie di notifiche CHANGE che portano a diverse query di database da diversi processi CA SDM, influendo in modo significativo sulle prestazioni di CA SDM.

Allo scopo di eliminare questo impatto sulle prestazioni CA SDM, è stato effettuato l'aggiornamento di dbmonitor_nxd per questo rilascio del prodotto. Il Monitor supporta un'interfaccia della riga di comando che consente all'utente di iniziare e terminare il monitoraggio di tabelle specifiche.

Sintassi

Il comando presenta il seguente formato:

```
dbmonitor_nxd  -c <command> -t <tables>
```

<command>

Fare clic su Avvia o Interrompi.

<tables>

Specifica un nome di tabella o un elenco delimitato da virgola di nomi di tabella che devono corrispondere a una o più delle tabelle specificate nella variabile di ambiente NX_DBMONITOR_TABLES.

Ciascuna richiesta viene inviata al daemon dbmonitor_nxd. Il daemon intraprende un'azione appropriata e restituisce un messaggio all'utente indicando l'azione intrapresa.

- Se viene invocata una richiesta di avvio per una tabella già avviata, non verrà intrapresa alcuna azione.
- Se viene invocata una richiesta di arresto per una tabella già terminata, non verrà intrapresa alcuna azione.
- Se il monitoraggio di una tabella viene avviato o terminato con successo, viene scritto anche un messaggio di registro in stdlog.

Nota: quando il monitor viene messo in pausa per una tabella, tutti i processi CA SDM che memorizzano nella cache i dati di queste tabelle potrebbero diventare obsoleti non verrà effettuato alcun aggiornamento di questa cache.

Ad esempio, BOPLGIN memorizza nella cache record di Contatto (dalle tabelle ca_contact e usp_contact) e questa cache non verrà aggiornata se il Monitor viene messo in pausa per la tabella ca_contact durante gli aggiornamenti esterni temporali caricati nel database. Nel caso di BOPLGIN ciò non influisce in modo significativo perché gli attributi essenziali di Contatto memorizzati nella cache in BOPLGIN vengono presi dalla tabella usp_contact e non dalla tabella ca_contact.

Nota: quando il monitoraggio di una tabella viene messo in pausa, gli utenti Web non potranno vedere, mentre visualizzano un modulo di dettaglio, i cambiamenti apportati esternamente alla tabella durante tale periodo di pausa.

pdm_backup - Scrittura di tabelle di database in file ASCII

Il comando pdm_backup arresta CA SDM, quindi scrive una o più tabelle di un database di CA SDM in un file ASCII. È possibile utilizzare questo file di output come file di input per il comando pdm_restore. Oltre al contenuto del database, il comando pdm_backup esegue anche il backup dei file di configurazione dell'applicazione.

Se si dispone di strumenti di backup specifici dell'ambiente operativo, si consiglia di utilizzarli al posto del comando pdm_backup. Dal momento che il comando pdm_backup è uno strumento generico, la sua esecuzione può risultare molto lenta su alcune combinazioni di ambiente operativo.

Nota: come parte del processo, l'utilità pdm_backup per prima cosa arresta i daemon (UNIX) o i servizi (Windows).

Sintassi

Il comando presenta il seguente formato:

```
pdm_backup [-d] [-g] [-v] -f nomefile [ALL | tabella1...tabellaN]
```

-d

Consente di specificare l'esecuzione del backup dei soli dati del database.

-g

Specifica che deve essere eseguito solo il backup dei dati non del database. Ciò significa che il backup riguarda solo i dati delle finestre (moduli) e altri elementi non di database.

-v

Specifica la modalità dettagliata, con la quale vengono scritti i commenti sull'esecuzione del comando nel file stdout.

-f *filename*

Specifica un file di output.

ALL|tabella1...tabellaN

Specifica tutti i file (ALL) oppure la tabella o le tabelle da scrivere. Se vengono specificate più tabelle, separarle con spazi.

- È possibile trovare nomi di tabelle nel file dello schema di database CA SDM, ddict.sch, presente in $NX_ROOT/sito (UNIX) o *directory di installazione*\sito (Windows). $NX_ROOT o *directory di installazione* rappresenta la directory in cui è stato installato CA SDM.
- Se non viene specificata alcuna tabella, viene scritto l'intero database di CA SDM, inclusi i gruppi di finestre e i file di registrazione dei menu.

Restrictions

Non è possibile eseguire il comando pdm_backup mentre CA SDM è attivo.

Importante: in UNIX, LIBPATH deve essere impostato prima di eseguire diverse utilità di CA SDM. Utilizzare *pdm_task* per impostare LIBPATH prima di eseguire un'utilità. Immettere ad esempio "pdm_task pdm_clean_attachments...".

Ulteriori informazioni:

pdm_restore - Ripristino di un database (a pagina 1157)

pdm_cache_refresh - Aggiornamento del database

Il comando pdm_cache_refresh forza i daemon o i processi di CA SDM a utilizzare i dati caricati nel database con l'utilità pdm_userload o altre utilità specifiche per database, inclusi gli strumenti per database non CA SDM.

La maggior parte dei daemon e dei file eseguibili di CA SDM mantiene i record del database caricati nella cache della memoria dinamica. Questa cache migliora le prestazioni eliminando la necessità di accedere al database quando i dati richiesti sono già disponibili. Quando il database viene aggiornato, la notifica si trasmette tra i file eseguibili di CA SDM. In questo modo, è possibile mantenere sempre aggiornata la cache. Tuttavia, questo tipo di notifica non viene ricevuta dalle utilità esterne, quali il comando pdm_userload o le utilità di database di terze parti. Se queste origini esterne caricano nuovi dati nel database, è necessario utilizzare il comando pdm_cache_refresh per notificare ai moduli di esecuzione di aggiornare la loro cache con le nuove informazioni del database.

Sintassi

Il comando presenta il seguente formato:

```
pdm_cache_refresh [-f nomefile] [-t elenco_tabelle] [-d] [-v]
```

-f filename

Specifica un file di testo che contiene un elenco delle tabelle di database che sono state modificate dall'esterno. Il file di testo può contenere una o più righe. Ciascuna riga specifica uno o più nomi di tabella separati da spazi.

-t elenco_tabelle

Specifica una o più tabelle modificate dall'esterno. Se l'elenco contiene più di una tabella, i nomi devono essere separati da punto e virgola (;) e l'intero elenco deve essere racchiuso tra virgolette. Le tabelle sono elencate nell'appendice "Dizionario degli elementi dei dati" della *Guida di riferimento tecnico*.

Ad esempio, si supponga di aver caricato i dati dell'ubicazione e del sito nel database di CA SDM utilizzando un'utilità di terze parti. Per indicare ai daemon di CA SDM di aggiornare la relativa cache, immettere il comando seguente:

```
pdm_cache_refresh -t "Location;Site"
```

-d

Invia un messaggio a domsrvr, il server del dominio CA SDM. Il server del dominio ricarica quindi gli elenchi di selezione, operazione che causa il lampeggiamento di qualsiasi finestra di elenco visualizzata sui client.

-v

Specifica la modalità dettagliata. Il valore 1 indica la modalità breve. Il valore 2 scrive i messaggi sull'esecuzione nel file di registro.

Importante: in UNIX, LIBPATH deve essere impostato prima di eseguire diverse utilità di CA SDM. Utilizzare *pdm_task* per impostare LIBPATH prima di eseguire un'utilità. Immettere ad esempio "pdm_task pdm_clean_attachments...".

pdm_configure - Apertura della finestra di configurazione

Il comando pdm_configure apre la finestra di configurazione di CA SDM. Utilizzare questa finestra per impostare la configurazione di CA SDM dopo l'installazione oppure per modificare la configurazione di CA SDM dopo l'esecuzione. Di seguito sono riportati i motivi possibili per modificare la configurazione di CA SDM:

- Modifica del tipo o del server di database
- Ricaricamento dei dati predefiniti
- Modifica delle password per gli account di sistema di CA SDM
- Rigenerazione dei file di schema per incorporare le modifiche
- Riconfigurazione del server seguente, a seconda della configurazione di CA SDM:
  - Convenzionale: server primario o secondario
  - Disponibilità avanzata: server applicazioni o in background

Sintassi

Il comando presenta il seguente formato:

```
pdm_configure
```

Restrictions

È possibile eseguire il comando pdm_configure su un server di CA SDM oppure su un client Linux di CA SDM. Per utilizzare il comando pdm_configure è necessario essere un utente con privilegi o root.

pdm_d_refresh - Avvio dei daemon con errori

L'utilità della riga di comando pdm_d_refresh viene utilizzata principalmente per le configurazioni dei daemon remoti. Indica al gestore dei daemon di riavviare i daemon il cui avvio non è riuscito per 10 volte e contrassegnati come "non eseguibili". Questa utilità contrassegna tutti i daemon come eseguibili e reimposta il contatore dei riavvii. A questo punto, il gestore dei daemon tenta l'avvio di tutti i daemon arrestati.

Sintassi

Il comando presenta il seguente formato:

```
pdm_d_refresh
```

Importante: in UNIX, LIBPATH deve essere impostato prima di eseguire diverse utilità di CA SDM. Utilizzare *pdm_task* per impostare LIBPATH prima di eseguire un'utilità. Immettere ad esempio "pdm_task pdm_clean_attachments...".

pdm_deref - Annullamento del riferimento (dati in formato ASCII)

Il comando pdm_deref elabora l'input in formato ASCII per scambiare i dati trovati in una tabella di database con i dati trovati in un'altra tabella di database. Può essere utilizzato per creare file compatibili con l'utilità pdm_userload da un database o foglio di lavoro non CA SDM. Può essere utilizzato anche per creare rapporti o file di output per database o fogli di lavoro non CA SDM.

Importante. Non utilizzare il comando pdm_deref se non si dispone delle conoscenze di linguaggio SQL necessarie. Le directory "export" e "import" in $NX_ROOT/samples (UNIX) o directory_installazione\samples (Windows) contiene un insieme di specifiche standard.

Sintassi

Il comando presenta il seguente formato:

```
nome pdm_deref –s file_specifiche [-c|-e|-r] [-d] [-h] [-n] [-u] [-v] <nomefile
```

-s file_specifiche

(Obbligatorio) Specifica un file che definisce quali dati devono essere scambiati e a quali condizioni.

file_specifiche contiene un elenco di comandi SQL nel formato seguente:

```
Deref

{
input = <elenco di attributi "from" dal file di input>
output = <elenco di attributi "to" per il file di output>
rule = "SELECT <atts used to fill output atts> \
  FROM <table name>  \
  WHERE <att from table name to match input 1> =?\
  AND <attributo da nome_tabella che deve corrispondere all'input 2> =? \
  OR <attributo da nome_tabella che deve corrispondere all'input 3> =?
}
```

-c

Genera output con valori separati da virgola, ad esempio:

```
"campo1","campo2","campo3"
```

Le opzioni per il formato di output -c, -e e -r si escludono a vicenda.

-e

Genera output in formato CSV (Comma-Separated Value, valori separati da virgola) con stringhe di dati racchiuse tra virgolette se contengono virgolette nel testo. Ad esempio:

```
"Stringa che contiene "virgolette" nel testo."
```

Le opzioni per il formato di output -c, -e e -r si escludono a vicenda.

-r

Genera output allineato a sinistra, se le etichette di colonna non vengono fornite nel file di input:

```
"etichetta":"valore"
```

o

```
"valore"
```

Questa opzione è indicata per le stampanti di linea, ad esempio:

```
Nome_campo: valore campo
```

Le opzioni per il formato di output -c, -e e -r si escludono a vicenda.

-d

Genera informazioni di diagnostica.

-h

Visualizza la Guida e le informazioni sulla sintassi.

-n

Specifica che le chiavi esterne con valore 0 non devono essere trattate come NULL. Questo argomento deve essere utilizzato solo in circostanze specifiche durante il recupero di un database danneggiato.

-u

Genera output senza intestazioni.

-v [1|2]

Specifica la modalità dettagliata. Il valore 1 indica la modalità breve. Il valore 2 scrive i messaggi sull'esecuzione nel file di registro.

filename

(Facoltativo) Specifica il file input in formato ASCII da elaborare. Se omesso, viene utilizzato stdin.

Limitazione—Valido solo in UNIX

Per utilizzare il comando pdm_deref in UNIX, la variabile di ambiente $NX_ROOT deve essere impostata sul percorso della directory di installazione di CA SDM e la variabile di ambiente PATH deve includere $NX_ROOT/bin.

Esempio: utilizzo di pdm_deref per impostare dati per l'input

L'esempio riportato di seguito illustra come utilizzare pdm_deref per impostare dati per l'input.

In base ai dati seguenti della tabella ca_location:

```
id    location_name_name
86873FA40BA4234A8CF7A418D7C8B2DB    "Boulder NCC"
```

E all'istruzione seguente nel file delle specifiche:

```
Deref
{
input = place
output = location_uuid
rule = "SELECT id FROM ca_location WHERE location_name=?"
}
```

Si desidera cambiare l'input seguente:

```
last_name, first_name, place
{"Potts", "Elmore", "Boulder NCC"}
```

Nell'output seguente, che può essere caricato nella tabella ca.contact con il comando pdm_userload:

```
last_name, first_name, location_uuid
{"Potts", "Elmore", "86873FA40BA4234A8CF7A418D7C8B2DB"}
```

Esempio: utilizzo di pdm_deref per impostare dati per l'output

L'esempio riportato di seguito illustra come utilizzare pdm_deref per impostare dati per l'output.

In base ai dati seguenti della tabella ca_contact:

```
id  last_name first_name
"69499D5A2424884887E62EC9823F5E47"    "Potts"    "Elmore"
```

E all'istruzione seguente nel file delle specifiche:

```
Deref
{
input = primary_contact_uuid
output = firstname, lastname
rule = "SELECT first_name, last_name FROM ca_contact
WHERE id=?"
}
```

Si desidera cambiare l'input seguente:

```
location_name, primary_contact_uuid
{"Boulder NCC", "69499D5A2424884887E62EC9823F5E47"}
```

nell'output seguente, che può essere stampato oppure inviato a un foglio di lavoro.

```
location_name, firstname, lastname
{"Boulder NCC", "Elmore", "Potts"}
```

Ulteriori informazioni:

pdm_extract - Estrazione dei dati dal database (a pagina 1134)

pdm_discimp - Importazione degli asset rilevati

Registrazione in batch degli asset non CA SDM rilevati. Questa utilità viene utilizzata per ricercare nell'MDB gli asset registrati da altri prodotti software e registrarli come asset CA SDM affinché possano essere utilizzati in CA SDM.

Funziona in modo simile alla finestra di dialogo Asset rilevati che può essere avviata dal modulo Web Ricerca asset/Elenco asset. Si tratta di un processo interattivo e in batch.

Questo programma eseguirà una query nelle tabelle ca_logical_asset, ca_asset e ca_logical_asset_property utilizzando diversi parametri e tenterà di registrare i nuovi asset CA SDM utilizzando i valori rilevati.

Sintassi

```
pdm_discimp [-l label] [-s serial number] [-t asset tag] [-n hostname] [-d dns name]
[-m mac address] [-c asset class] [-v] [-r] [-o object manager]
```

Criteri di selezione degli asset (utilizzare % come carattere jolly):

l

Trova l'etichetta asset specificata.

s

Trova il numero di serie specificato.

t

Trova il tag asset specificato.

n

Trova il nome host specificato.

Criteri di selezione delle proprietà degli asset (utilizzare % come carattere jolly):

d

Trova il nome DNS specificato.

m

Trova l'indirizzo mac specificato.

Altre opzioni:

c

Classe asset da assegnare quando la registrazione predefinita per i nuovi asset proprietari è Hardware rilevato.

v

Modalità dettagliata/diagnostica.

r

Registra gli asset. In caso contrario, viene eseguito in modalità simulazione.

h

Visualizza la Guida (queste informazioni).

o

Gestore oggetti (domsrvr) da utilizzare per l'elaborazione.

Nota: se l'elaborazione restituisce un'etichetta asset vuota, per l'etichetta verrà utilizzato il valore trovato per il nome host o il nome DNS. È necessario che gli asset abbiano almeno un'etichetta e una classe asset da registrare per l'uso in CA SDM.

A causa delle limitazioni della struttura dell'MDB e dell'architettura di CA SDM, vengono eseguite due query per selezionare i record appropriati per l'elaborazione. Si tratta di un particolare fondamentale perché può condizionare le prestazioni. La prima query recupera dalle tabelle ca_logical_asset e ca_asset le righe corrispondenti all'etichetta, al numero di serie, al tag e al nome host. Quindi, per ciascuna riga risultante, viene eseguita una query nella tabella ca_logical_asset_property per verificare la corrispondenza per nome_dns e indirizzo_mac. L'asset rilevato dalla prima query viene selezionato per la registrazione se la seconda query restituisce delle righe.

Importante: in UNIX, LIBPATH deve essere impostato prima di eseguire diverse utilità di CA SDM. Utilizzare *pdm_task* per impostare LIBPATH prima di eseguire un'utilità. Immettere ad esempio "pdm_task pdm_clean_attachments...".

pdm_discupd -- Aggiornamento asset rilevati

Registrazione in batch degli asset non CA SDM rilevati. Utilizzare questa utilità per aggiornare asset importati dal comando pdm_discimp.

Sintassi

```
pdm_discupd [-t] [-v] [-d domsrvr]
```

in cui:

t

Test

v

Modalità dettagliata/diagnostica.

d

Gestore oggetti (domsrvr) da utilizzare per l'elaborazione.

Importante: in UNIX, LIBPATH deve essere impostato prima di eseguire diverse utilità di CA SDM. Utilizzare *pdm_task* per impostare LIBPATH prima di eseguire un'utilità. Immettere ad esempio "pdm_task pdm_clean_attachments...".

pdm_extract - Estrazione dei dati dal database

Il comando pdm_extract estrae i dati dalle tabelle di database CA SDM specificate oppure dall'intero database CA SDM generando l'output come testo in formato ASCII.

Sintassi

Il comando presenta il seguente formato:

```
pdm_extract [-c|-e|-r] [-d] [-h] [-u] [-v] [-C] --B] [-f stringaformato| ALL | tabella1
. . . tabellaN]
```

-c

Genera output con valori separati da virgola, ad esempio:

```
"campo1","campo2","campo3"
```

Le opzioni per il formato di output -c, -e e -r si escludono a vicenda.

-e

Genera output in formato CSV (Comma-Separated Value, valori separati da virgola) con stringhe di dati racchiuse tra virgolette se contengono virgolette nel testo. Ad esempio:

```
"Stringa che contiene "virgolette" nel testo."
```

Le opzioni per il formato di output -c, -e e -r si escludono a vicenda.

-r

Genera output allineato a sinistra, se le etichette di colonna non vengono fornite nel file di input:

```
"etichetta":"valore"
```

o

```
"valore"
```

Questa opzione è indicata per le stampanti di linea, ad esempio:

```
Nome_campo: valore campo
```

Le opzioni per il formato di output -c, -e e -r si escludono a vicenda.

-d

Utilizza il formato data trovato nel file $NX_ROOT/fig/english/cfg/dataent.fmt (UNIX) o in *directory_installazione*\fig\english\cfg\dataent.fmt (Windows). Il file può essere modificato in base alle proprie necessità.

-h

Visualizza la Guida e le informazioni sulla sintassi.

-u

Genera output senza intestazioni.

-v

Specifica la modalità dettagliata, con la quale vengono scritti i commenti sull'esecuzione del comando nel file stdout.

-C

Modifica la codifica da UTF-8 a un altro set di caratteri. L'output predefinito è UTF-8.

Esempio: per convertire l'output in JIS, è necessario eseguire "-C iso-2022-jp"

Esempio: per la codifica nel set di caratteri nativo del sistema operativo, usare "DEFAULT" o "NATIVE".

-B

Sopprime il Byte Order Mark se è impostata la variabile NX_ADD_UTF8_BYTE_ORDER_MARK.

L'opzione NX_ADD_UTF8_BYTE_ORDER_MARK è una firma in un file. Consente editor che supportano UTF-8 per gestire l'integrità UTF-8 del file.

Nota: questo è necessario solo per dati non-ASCII. Se non viene installato, il comportamento predefinito omette il Byte Order Mark (BOM). Se installato, impostarlo su "1" o "Sì".

-f *stringaformato*

Estrae record e campi specifici in base al valore di *formato* (un sottoinsieme di istruzioni SQL).

Per specificare una data dopo un periodo, utilizzare la seguente sintassi:

pdm_extract -v -f "select id, ref_num from Call_Req where open_date >= DATE '2005-02-24'" > daterange1.txt

Per specificare un intervallo di date, utilizzare la seguente sintassi:

pdm_extract -v -f "select id, ref_num from Call_Req where open_date >= DATE '2004-01-20' and open_date < DATE '2004-02-25'" > daterange2.txt

Nota: racchiudere il formato YYYY-MM-DD tra apici.

La sintassi per DATE è la seguente:

```
DATE 'yyyy-mm-dd'
```

yyyy = numero intero che rappresenta l'anno (tra il 1970 e il 2038)

mm = numero intero che rappresenta il mese

dd = numero intero che rappresenta il giorno

Esempi:

```
DATE '2005-01-18'
DATE '1999-12-25'
```

La sintassi dell'istruzione TIMESTAMP è:

```
TIMESTAMP 'yyyy-mm-dd hh.mm.ss[.nnnnnn][[+|-][hh.mm]]
```

yyyy = numero intero che rappresenta l'anno (tra il 1970 e il 2038)

mm = numero intero che rappresenta il mese

dd = numero intero che rappresenta il giorno

hh = numero intero che rappresenta l'ora

mm = numero intero che rappresenta i minuti

ss = numero intero che rappresenta i secondi

nnnn = (opzionale) numero intero che rappresenta le frazioni di secondo

[+|-][hh.mm] = (opzionale) fuso orario.

Esempi:

```
TIMESTAMP '1998-04-28 12:00:00.000000'
TIMESTAMP '2004-10-17 18:30:45'
TIMESTAMP '2005-03-21 12:00:12+08:00'
TIMESTAMP '1999-05-10 09:12:23.005-03:30'
```

Nota: l'opzione -d non è obbligatoria poiché influenza unicamente il formato dell'output.

Di seguito presentiamo un esempio di utilizzo del comando:

```
pdm_extract -f "select * from Call_Req where open_date > TIMESTAMP '2004-01-12
12:00:00'"
```

In questo esempio, tutte le colonne vengono estratte dalla tabella Call_Req, dove il valore di open_date è successivo alla mezzanotte del giorno 1/12/2004.

TUTTO

Estrae l'output da tutte le tabelle del database.

```
tabella1 . . tableN
```

Estrae l'output dalle tabelle specificate. I nomi di tabella devono essere separati da spazi.

Se non viene specificato un formato, il formato predefinito è un file ASCII compatibile con pdm_userload.

Ulteriori informazioni:

pdm_deref - Annullamento del riferimento (dati in formato ASCII) (a pagina 1128)
pdm_replace - Sostituzione di una tabella di database (a pagina 1154)
pdm_userload - Aggiunta, aggiornamento ed eliminazione dei record del database (a pagina 1166)
rpt_srv - Generazione dei rapporti (a pagina 1174)

pdm_halt - Arresto dei daemon o dei servizi

Il comando pdm_halt arresta immediatamente tutti i daemon CA SDM (UNIX) o il servizio server di sistema (Windows) sul sistema su cui viene eseguito. Solitamente, il tempo di completamento dell'utilità pdm_halt è di circa 30 secondi. Se l'esecuzione si protrae per oltre 2 minuti, premere Ctrl+C per arrestare l'utilità pdm_halt e riprovare.

Sintassi

Il comando presenta il seguente formato:

```
pdm_halt [-w] [-a] [time]
```

-w

Attende l'interruzione del daemon.

-a

Interrompe tutti i proctor definiti nel file pdm_startup.

[time]

Specifica il numero di secondi da attendere prima dell'esecuzione del comando.

Restrictions

È possibile eseguire il comando pdm_halt su un server CA SDM oppure su un client UNIX su cui è installato CA SDM. Per utilizzare il comando pdm_halt, è necessario disporre dei privilegi appropriati.

pdm_init - Avvio dei daemon

Valido solo per l'ambiente UNIX.

Il comando pdm_init avvia tutti i processi automatici di CA SDM sul sistema su cui viene eseguito. Questi processi automatici sono chiamati *daemon* e sono sempre in esecuzione in background mentre si lavora. Non tutti i daemon vengono avviati. Alcuni di essi sono specifici per determinati sistemi operativi. Vedere il capitolo sulla gestione dei server per un elenco di daemon avviabili da questo comando.

Nota: utilizzare il comando pdm_d_refresh per avviare i daemon il cui avvio non è riuscito la prima volta (deve essere stato però prima risolto il problema che ne ha impedito l'avvio la prima volta). Nella maggior parte dei casi non è necessario arrestare i daemon per avviare quelli la cui prima esecuzione non era riuscita.

Sintassi

```
pdm_init
```

Restrictions

È possibile eseguire il comando pdm_init su un server CA SDM oppure su un client UNIX su cui è installato CA SDM. Per utilizzare il comando pdm_init è necessario essere un utente con privilegi.

pdm_key_refresh - Aggiornamento delle informazioni chiave nella cache

L'utilità pdm_key_refresh aggiorna le informazioni chiave inserite nella cache dalla tabella di controllo chiave nel database. Se si aggiornano le informazioni di controllo chiave, è possibile eseguire questa utilità invece di arrestare e riavviare il sistema per forzare CA SDM a utilizzare il nuovo valore basato sull'ID chiave.

Importante. La modifica della tabella di controllo chiave può danneggiare i dati. Si consiglia di non tentare di modificare il controllo chiave senza istruzioni specifiche del Supporto tecnico di CA.

Sintassi

Il comando presenta il seguente formato:

```
pdm_key_refresh
```

Importante: in UNIX, LIBPATH deve essere impostato prima di eseguire diverse utilità di CA SDM. Utilizzare *pdm_task* per impostare LIBPATH prima di eseguire un'utilità. Immettere ad esempio "pdm_task pdm_clean_attachments...".

pdm_lexutil--Modifica del dizionario di CA SDM

L'utilità pdm_lexutil consente di modificare il dizionario di Service Desk, oltre ad aggiungere o eliminare parole per il dizionario del correttore ortografico.

Sintassi

Il comando presenta il seguente formato:

```
pdm_lexutil -a | -d [-f] [-l] wordlist
```

-a

Aggiunta di parole.

-d

Eliminazione di parole.

-f

File o dizionario contenente un elenco di parole da aggiungere o eliminare.

-l

Nome del dizionario.

Predefinito: userdict.tlx

wordlist

Parole da aggiungere o eliminare.

Importante: in UNIX, LIBPATH deve essere impostato prima di eseguire diverse utilità di CA SDM. Utilizzare *pdm_task* per impostare LIBPATH prima di eseguire un'utilità. Immettere ad esempio "pdm_task pdm_clean_attachments...".

pdm_k_reindex—Utilità di reindicizzazione della conoscenza

L'utilità di reindicizzazione della conoscenza, pdm_k_reindex.exe, si trova nella directory di installazione di Gestione della conoscenza.

Nota: La reindicizzazione dei documenti nell'archivio della conoscenza può richiedere molto tempo, a seconda delle dimensioni del database. Pertanto, si consiglia di eseguire l'utilità di reindicizzazione della conoscenza solo dopo aver apportato tutti i cambiamenti. Per la configurazione con disponibilità avanzata, non è possibile eseguire l'utilità di reindicizzazione della conoscenza durante il failover.

Importante. Su UNIX, è necessario impostare LIBPATH prima di eseguire varie utilità di CA SDM. Utilizzare pdm_task per impostare LIBPATH prima di eseguire un'utilità. Ad esempio, immettere "pdm_task pdm_clean_attachments ...".

Procedere come descritto di seguito:

1. Aprire un prompt dei comandi.
2. Immettere il comando seguente nel prompt dei comandi per eseguire la reindicizzazione della conoscenza:

Ad esempio:

```
pdm_k_reindex
```

Le opzioni seguenti sono disponibili con questo comando.

-D

Definisce la modalità di debug, ad esempio la stampa sulla finestra di comando.

-v

Definisce la modalità dettagliata, ad esempio la stampa nel file stdlog.

-i

Non crea indici di tabella nella tabella di reindicizzazione dopo tale operazione.

Nota: I parametri il cui prefisso contiene un trattino, ad esempio "-D", devono precedere gli altri parametri.

L'altra opzione è la seguente:

***File*:reindex.txt**

I documenti vengono reindicizzati nel file specificato.

+i

Crea solo gli indici della tabella di reindicizzazione, che diventerà la tabella di ricerca dopo l'esecuzione della reindicizzazione. Gli indici precedenti vengono eliminati prima della reindicizzazione.

+t

Cambia solo i nomi della tabella di ricerca e della tabella di reindicizzazione.

Nota: il prefisso "+" indica che verrà applicato solo il parametro ad esso associato.

sdtout

Consente di specificare la frequenza con cui vengono visualizzate le informazioni statistiche nella finestra del comando. Per impostazione predefinita, l'utilità di reindicizzazione della conoscenza fornisce informazioni statistiche nella finestra dei comandi per ogni 1000 documenti elaborati. Talvolta, tuttavia, viene richiesto di fornire le statistiche con maggiore frequenza. Utilizzare il parametro:

```
pdm_k_reindex -i sdtout:10
```

In questo caso, le statistiche vengono visualizzate nella finestra di comando dopo l'elaborazione di dieci documenti.

I documenti vengono reindicizzati nell'archivio della conoscenza.

Modalità di utilizzo di pdm_k_reindex

Eseguire l'utilità pdm_k_reindex se vengono modificate una o più delle impostazioni di ricerca seguenti:

- Parole non significative
- Sinonimi
- Termini speciali
- Lingua
- Rimuovi parole simili

- Rimuovi parole non significative
- Intervallo caratteri validi
- Riconosci termini speciali

Quando si applica un cambiamento, viene visualizzato un apposito messaggio nel nodo Conoscenza della scheda Amministrazione.

Tracciamento del processo di reindicizzazione

Mentre il processo di reindicizzazione è in corso, è possibile esaminarne lo stato nell'apposita sezione che si trova nella parte inferiore della pagina. Di seguito è riportata la descrizione di ciascun campo:

N. documenti

Indica il numero di documenti già elaborati.

Dimensioni medie (Parole)

Indica le dimensioni dei documenti correnti. Questo valore viene calcolato sottraendo al numero di parole totale il numero di parole non significative.

Classificazione (Doc/Sec)

Indica il numero di documenti elaborati al secondo.

Tempo dall'avvio

Indica il tempo trascorso dall'avvio del processo di reindicizzazione.

Tempo restante

Indica la quantità di tempo restante stimata per il processo, basata sulla frequenza corrente e sul numero di documenti restanti.

N. errori

Indica il numero di documenti con errori (massimo=100). Quando viene raggiunto il numero massimo di documenti con errori, viene richiesto se continuare l'esecuzione del processo o annullarla.

Nota: se sono stati apportati cambiamento a Parole di disturbo, Termini speciali, Sinonimi o Impostazioni di analisi ma non è stata eseguita la reindicizzazione, questa operazione viene richiesta al successivo accesso al nodo Conoscenza della scheda Amministrazione. I cambiamenti saranno effettivi solo dopo aver eseguito l'utilità Knowledge Reindex.

Importazione e reindicizzazione

Quanto viene richiamata dalla riga di comando, l'utilità pdm_kit importa i documenti nel database. Al termine dell'esecuzione, viene automaticamente richiamata l'utilità di reindicizzazione (pdm_k_reindex.exe) se l'indicizzazione o la reindicizzazione dei documenti non è stata disabilitata tramite le apposite opzioni della riga di comando. Lo stato e l'output dell'operazione di reindicizzazione viene automaticamente scritto nel file "EBR_REINDEX.LOG" nella directory $NX_ROOT\log.

Indicizzazione e deindicizzazione di impostazioni della coda per l'elaborazione batch e istantanea

Le funzionalità di indicizzazione e deindicizzazione eseguono entrambe un processo batch per includere un numero predefinito di documenti in una sola operazione. Questi processi batch servono per ottimizzare le prestazioni. Più documenti si includono nel batch e migliori saranno le prestazioni del sistema.

Il numero di documenti che è possibile elaborare è limitato. Tale limite dipende dalle dimensioni dei documenti e degli allegati collegati. Le dimensioni del documento vengono calcolate in base al solo testo e ai suo allegati. Gli elementi relativi alle immagini e al formato non vengono inclusi nel calcolo.

Nota: è possibile limitare la dimensione degli allegati utilizzando Libreria allegati, Repository nella scheda Amministrazione e modificando il repository per definire la dimensione limite del file per l'archivio della conoscenza (KB).

Le dimensioni massime consigliate per il batch sono comprese tra 2 e 12 MB (in base al parametro EBR_MAX_INDEX_BATCH_SIZE del file NX.env e alle dimensioni medie del documento).

- Se le dimensioni medie del documento (compresi gli allegati) è circa 0,1 MB, è opportuno mantenere l'impostazione predefinita in NX.env:

  ```
  @EBR_MAX_INDEX_BATCH_SIZE=128
  @NX_EBR_INDEX_QUEUE_TIMEOUT=10
  @NX_EBR_REINDEX_QUEUE_TIMEOUT=1
  @NX_EBR_INDEX_QUEUE_ONLINE=Yes
  @NX_EBR_NON_KD_INDEX_QUEUE_ONLINE=Yes
  ```

  Questa impostazione indica che un batch elabora 128 documenti, che i batch vengono eseguiti ad intervalli di dieci secondi e che, in caso di reindicizzazione, il tempo di attesa tra due batch è un secondo.

- Se le dimensioni medie del documento (compresi gli allegati) è circa 0,5 MB, è opportuno mantenere l'impostazione predefinita in NX.env

  ```
  @EBR_MAX_INDEX_BATCH_SIZE=25
  @NX_EBR_INDEX_QUEUE_TIMEOUT=10
  @NX_EBR_REINDEX_QUEUE_TIMEOUT=10
  @NX_EBR_INDEX_QUEUE_ONLINE=No
  @NX_EBR_NON_KD_INDEX_QUEUE_ONLINE=No
  ```

  Questa impostazione indica che un batch elabora 25 documenti, che i batch vengono eseguiti ad intervalli di dieci secondi e che, in caso di reindicizzazione, il tempo di attesa tra due batch è un secondo.

pdm_listconn - Elenco delle connessioni attive

È possibile utilizzare il comando pdm_listconn per elencare le connessioni attive sui client e sui server.

Sintassi

Il comando presenta il seguente formato:

```
pdm_listconn [-c] [-s] [–s -c] [–t nn] [proc1 [proc2...]]
```

Il comando predefinito segue il formato seguente se non viene specificato alcun parametro:

```
pdm_listconn -s -t 2
```

-c

Elenca le connessioni per client. Il comando visualizza due righe per ciascun client:

(*n* sec) *tipo_client nodo*|*procc*

connected to *alias* (*procs*) at *ora*

n è il numero di secondi impiegati dal client per la risposta.

tipo_client è "vbop", "animator daemon" o "web engine".

nodo è l'indirizzo IP del nodo del client.

procc è il nome del processo slump del client.

alias è l'alias del server a cui è connesso il client.

procs è il nome del processo slump del server.

ora è il tempo di connessione.

Ad esempio:

```
(0 sec) vbop client 141.202.211.34|vbop-0x40120000:anthill:0
         connected to CMD40120 on anthill (domsrvr) at 19/02/99 10:44:16
```

-s

Elenca le connessioni per server (impostazione predefinita). Il comando visualizza due righe per ciascun server:

(*n* secs) server *alias* (*node*|*procs*) willingness *disponibilità*
numero client connessi (utilizzare pdm_listconn -c -s per elencare i client per server)

n è il numero di secondi impiegati dal server per la risposta.

nodo è l'indirizzo IP del nodo del server.

alias è l'alias del server a cui è connesso il client.

procs è il nome del processo slump del server.

disponibilità è la disponibilità del server ad accettare nuovi client (0 - 100).

numero corrisponde al numero di client connessi.

Ad esempio:

```
(0 sec) server CMD40120 on anthill (domsrvr) willingness 98
2 connected clients (utilizzare pdm_listconn -c -s per elencare i client per
server)
   vbop client 141.202.211.34|vbop2 connected 19/02/99 10:53:16
   vbop client 141.202.211.34|vbop-0x40120000:anthill:0 connected 19/02/99
10:44:17
```

-s -c

Elenca le connessioni per server, inclusi i dettagli del client per ciascun server. Il comando visualizza diverse righe per ciascun server:

(*n* secs) server *alias* (*node*|*procs*) willingness *disponibilità*
numero connected clients:
client_type node|cproc connected time

dove:

n è il numero di secondi impiegati dal server per la risposta.

nodo è l'indirizzo IP del nodo del server.

alias è l'alias del server a cui è connesso il client.

procs è il nome del processo slump del server.

disponibilità è la disponibilità del server ad accettare nuovi client (0 - 100).

numero corrisponde al numero di client connessi.

tipo_client è "vbop", "animator daemon" o "web engine".

nodo è l'indirizzo IP del nodo del client.

procc è il nome del processo slump del client.

ora è il tempo di connessione.

Ad esempio:

```
(0 sec) server CMD40120 on anthill (domsrvr) willingness 98
2 connected clients:
    vbop client 141.202.211.34|vbop2 connected 19/02/99 10:53:16
    vbop client 141.202.211.34|vbop-0x40120000:anthill:0 connected 19/02/99
10:44:17
```

-t nn

Specifica un intervallo di timeout in secondi. Poiché pdm_listconn riceve informazioni da un numero sconosciuto di client e server, termina quando scade l'intervallo di timeout specificato dopo la ricezione dell'ultimo messaggio.

Impostazione predefinita: 2

proc1

Specifica uno o più nomi di processo slump, separati da spazi. L'utilità visualizza informazioni sul client o sul server.

Importante: in UNIX, LIBPATH deve essere impostato prima di eseguire diverse utilità di CA SDM. Utilizzare *pdm_task* per impostare LIBPATH prima di eseguire un'utilità. Immettere ad esempio "pdm_task pdm_clean_attachments...".

pdm_load - Aggiunta, aggiornamento ed eliminazione dei record del database

Importante. L'uso di pdm_load può essere distruttivo, quindi è necessario effettuare sempre il backup del database prima di eseguire pdm_load e utilizzare pdm_userload a meno che non venga richiesto di usare pdm_load.

Il comando pdm_load aggiorna il database di CA SDM utilizzando un file di input specificato dall'utente che contiene un massimo di 112 attributi.

Ogni volta che i ticket vengono caricati (ad esempio, Richieste o Issue), il numero di ticket deve includere un prefisso o un suffisso univoco nella propria stringa. CA SDM interpreta questo numero come stringa di caratteri e non come numero sequenziale. Pertanto, non viene assicurata l'assegnazione di un numero univoco ai ticket caricati. Se si assegna un prefisso o un suffisso univoco utilizzando Awk o un altro programma di elaborazione testi, è possibile caricare i ticket con la sicurezza che CA SDM non sovrascriva i ticket già esistenti.

Sintassi

Il comando presenta il seguente formato:

```
pdm_load [-c] [-h] [-m] [-r] [-u] [-v] –f nomefile
```

Il formato degli elementi del file di input è il seguente:

```
TABLE nome_tabella
nomecampo1 nomecampo2 . . . . nomecampoN
{ "value11", "value12", . . . "value1N" }
{ "value21", "value22", . . . "value2N" }
.
.
.
{ "valueN1", "valueN2", . . . "valueNN" }
```

table_name è il nome della tabella da caricare, indicato nel file dello schema del database di CA SDM, ubicato in $NX_ROOT/site/schema.sch (UNIX) or *installation-directory*\site\schema.sch (Windows). $NX_ROOT o *directory di installazione* rappresenta la directory in cui è stato installato CA SDM.

-f *filename*

Specifica il file di input in formato ASCII.

-c

Controlla il file di input con il database e segnala gli aggiornamenti necessari, ma non applica gli aggiornamenti.

-m

Specifica l'aggiornamento di massa. Specificare questo parametro quando si deve aggiungere o eliminare un numero elevato di record. Questa opzione sopprime tutte le notifiche ai client relative agli aggiornamenti e invia un messaggio che indica di aggiornare la cache di una tabella quando il comando pdm_load termina di elaborarla.

-r

Rimuove i record dal database che corrispondono ai record di input.

Importante. Creare una copia di backup del database prima di eseguire il comando pdm_load con questa opzione. Una volta rimossi i vecchi record dal database, per recuperare gli eventuali record eliminati è necessario ripristinare il database di CA SDM con questa copia di backup.

-u

Aggiorna i record esistenti, ma non inserisce nuovi record nel database.

Ulteriori informazioni:

pdm_replace - Sostituzione di una tabella di database (a pagina 1154)
pdm_userload - Aggiunta, aggiornamento ed eliminazione dei record del database (a pagina 1166)
pdm_backup - Scrittura di tabelle di database in file ASCII (a pagina 1124)
pdm_restore - Ripristino di un database (a pagina 1157)

pdm_logfile - Modifica delle dimensioni cutover del file stdlog

Il comando pdm_logfile consente di modificare le dimensioni cutover del file stdlog.*x*. Il cutover si può verificare dopo la scrittura di un numero specificato di byte. In UNIX, questo valore viene ripristinato ogni volta che si esegue il comando pdm_init. In Windows, le impostazioni vengono mantenute ogni volta che si eseguono i comandi pdm_halt e pdm_init.

Sintassi

Il comando presenta il seguente formato:

```
pdm_logfile [-L|-h]
```

o

```
pdm_logfile [-g -h] [-b byte]
```

Esempio

Per impostare il cutover dei file stdlog.*x* ogni 500.000 byte, immettere il comando seguente:

```
pdm_logfile -f STD -b 500000
```

-L

Crea un elenco dei cutover correnti.

-q

Esegue il comando pdm_logfile in modalità non interattiva.

-b byte

Specifica il numero di byte che devono essere scritti prima del cutover.

Restrictions

È possibile eseguire il comando pdm_load mentre CA SDM è attivo, tuttavia le prestazioni potrebbero risentirne in modo significativo. Si consiglia di eseguire il comando pdm_load quando nessun utente sta utilizzando CA SDM.

Importante: in UNIX, LIBPATH deve essere impostato prima di eseguire diverse utilità di CA SDM. Utilizzare *pdm_task* per impostare LIBPATH prima di eseguire un'utilità. Immettere ad esempio "pdm_task pdm_clean_attachments...".

Utilità pdm_log4j_config - Modifica del file delle proprietà log4j

L'utilità pdm_log4j_config consente di configurare i file delle proprietà log4j di CA SDM, i componenti Web, PDM_RPC, Support Automation, Resto e CMDB Visualizer. Esegue lo script in batch dell'utilità adatto al proprio ambiente. Per Windows, eseguire pdm_log4j_config dalla riga di comando. Per UNIX, eseguire il file pdm_log4j_config.sh.

Il comando presenta il seguente formato:

```
pdm_log4j_config –f <component> -d
pdm_log4j_config -h
pdm_log4j_config –f <component>  [-a | -n <name>] [-l <log level>] [I <max # of log
files>] [-s <max size of log files>] [-t <log level threshold>]
```

-f

Specifica la configurazione log4j di CA SDM o il componente di CA SDM che si desidera modificare. Immettere uno dei valori seguenti:

SDM_WEB, SDM_RPC, REST, SA, o Viz.

Nota: utilizzare l'opzione obbligatoria con le altre opzioni.

-d

Visualizza la configurazione corrente di log4j.properties.

-h

Visualizza la Guida in linea dell'utilità.

-a

Completa tutte le modifiche a log4j.properties a livello globale.

-n

Specifica la modifica di un nome di classe o di pacchetto specifico.

Specificare un nome di classe, ad esempio bop_logging, oppure un nome di pacchetto completo, ad esempio com.ca.ServicePlus.

-l

Specifica il livello di registro che si desidera impostare.

Nota: specificare l'opzione di -a oppure -n.

-i

Specifica l'indice di numero di file massimo che si desidera impostare.

Nota: specificare l'opzione di -a oppure -n.

-s

Specifica le dimensioni di file massime che si desidera impostare.

Nota: specificare l'opzione di -a oppure -n.

Importante. Modificare l'appender nel file log4j.properties del Visualizer in Rolling File Appender prima di eseguire il comando con questo parametro. Se non si modifica l'appender, MaxFileSize genera registri nello stesso file.

-t

Specifica la soglia del livello di registro.

Nota: specificare l'opzione di -a oppure -n.

Esempi di uso dell'utilità

L'elenco seguente fornisce alcuni esempi di utilizzo dell'utilità pdm_log4j_config:

- Modifica del livello di dettaglio del registro per tutti i logger configurati nel file delle proprietà mediante le variabili -l e -a.

  Ad esempio, è possibile impostare tutti i logger configurati in Support Automation a un livello di DEBUG:

  ```
  pdm_log4j_config –f SA -a -l DEBUG
  ```

- Modifica del livello di dettaglio del registro per una classe di logger o un nome di pacchetto specifico nel file delle proprietà log4j di CA SDM mediante le variabili -l e -n.

  Ad esempio, è possibile impostare il logger per il pacchetto pdm_rpc su DEBUG utilizzando uno dei seguenti codici di esempio:

  ```
  pdm_log4j_config –f SDM_RPC -n pdm_rpc -l DEBUG
  ```

  ```
  pdm_log4j_config –f SDM_RPC -n com.ca.ServicePlus.pdm_rpc -l DEBUG
  ```

- Modificare il numero massimo di file di registro da creare per tutti gli appender (proprietà MaxBackupIndex) utilizzando le variabili -i e -a nel file delle proprietà log4j di REST.

  Ad esempio, impostare 9 come numero massimo di file per tutti gli appender.

  ```
  pdm_log4j_config –f REST -a -i 9
  ```

- Modifica del numero massimo di file di registro configurati nel file delle proprietà log4j di CA SDM per la creazione di un appender per una classe specifica o un insieme di classi (proprietà MaxBackupIndex) mediante le variabili -i e -n.

  Ad esempio, è possibile impostare 7 come numero massimo di file per bop_logging.

  ```
  pdm_log4j_config –f SDM_WEB -n bop_logging -i 7
  ```

- Modifica delle dimensioni massime di ciascun file di registro configurato nel file delle proprietà log4j di REST per la creazione degli appender (proprietà MaxFileSize) mediante le variabili -s e -a.

  Ad esempio, è possibile impostare 9 come dimensione massima dei file per tutti gli appender.

  ```
  pdm_log4j_config –f REST -a -s 9MB
  ```

- Modifica delle dimensioni massime dei file di registro configurati nel file delle proprietà log4j di CA SDM per la creazione di un appender per una classe specifica o un insieme di classi (proprietà MaxFileSize) mediante le variabili -s e -n.

  Ad esempio, è possibile impostare 7 come dimensione massima di bop_logging.

  ```
  pdm_log4j_config –f SDM_WEB -n bop_logging -s 7MB
  ```

- Modifica della soglia del livello di registro per tutti gli appender configurati nel file delle proprietà dlog4j di Support Automation (proprietà di soglia) mediante le variabili -t e -a.

  Ad esempio, è possibile impostare la soglia del livello di registro su DEBUG.

  ```
  pdm_log4j_config –f SA -a -t DEBUG
  ```

  Nota: il parametro -t della soglia del livello di registro prevale sul parametro -l del livello di registro. In caso di modifica del livello di registro e del livello di soglia, i registri di debug del servlet non verranno visualizzati nel file.

- Modifica della soglia del livello di registro per un appender per una classe specifica o un insieme di classi (proprietà di soglia) configurato nel file delle proprietà log4j di CA SDM mediante le variabili -t e -n.

  Ad esempio, è possibile impostare la soglia del livello di registro su WARN.

  ```
  pdm_log4j_config –f SDM_WEB -n bop_logging -t WARN
  ```

- Esecuzione del comando seguente per la visualizzazione della configurazione del logger e dell'appender corrente nel file delle proprietà log4j di REST:

  ```
  pdm_log4j_config –f REST -d
  ```

Importante. Utilizzare le variabili -l, -i, -s, e -t insieme a una delle opzioni -a o -n, ma non utilizzare entrambe le opzioni. L'opzione -f è obbligatoria. Le opzioni -h e -d sono escludono automaticamente qualsiasi altra opzione.

Modifica manuale dell'intervallo di aggiornamento del file di registro

Gli amministratori possono modificare l'intervallo di monitoraggio delle modifiche del file log4j.properties. Per impostazione predefinita, l'intervallo di aggiornamento è impostato ogni 60 secondi. I componenti di CA SDM, inclusi i servlet SDM, PDM_RPC, Support Automation, CMDB Visualizer e REST eseguono la connessione mediante il file log4j.

Procedere come descritto di seguito:

1. Aprire la directory seguente sul server CA SDM:

   ```
   NX_ROOT
   ```

2. Aprire il file NX.env per la modifica.
3. Modificare la variabile NX_LOG4J_REFRESH_INTERVAL con un valore in millisecondi.

   Nota: se il valore immesso è negativo o non numerico, verrà utilizzato il valore predefinito di 60 secondi.

4. Salvare il file NX.env.

Modifica dell'appender jsrvr.log

Per impostazione predefinita, i servlet quali PDMContextListener, pdmweb, UploadServlet e pdm_report registrano i messaggi di livello INFO nel file jsrvr.log. Modificare il livello di soglia dell'appender jsrvr.log per eseguire la registrazione di qualsiasi messaggio del livello INFO.

Procedere come descritto di seguito:

1. Modificare il livello nel file log4j.properties con la seguente soglia:

   ```
   log4j.appender.jsrvrlog.Threshold=debug
   ```

2. Modifica il livello di registro di UploadServlet:

   ```
   log4j.logger.com.ca.ServicePlus.uploadservlet=debug, jsrvrlog
   ```

3. Aprire il file jsrvr.log.
4. Confermare che i messaggi di livello DEBUG di UploadServlet vengano visualizzati.

Nota: in caso di modifica del livello di registro ma non del livello di soglia, i registri DEBUG del servlet non verranno visualizzati nel file. Non tutti i servlet dispongono di logger espliciti associati. Ad esempio, il file log4j.properties include pdmweb, BOServlet, pdm_export, pdm_report e pdm_cache appartenenti al servlet pdmweb. Per visualizzare i registri di debug da questi servlet, modificare il livello di registro pdmweb.

Modifica dell'appender jstd.log

Tutti i registri delle applicazioni nonwebapp vengono aggiunti al file jstd.log separatamente. Per visualizzare i registri per tali applicazioni, ad esempio pdm_rpc, modificare il livello di registro dell'applicazione desiderata.

Procedere come descritto di seguito:

1. Modificare il seguente livello di registro:

   ```
   log4j.logger.com.ca.ServicePlus.pdm_rpc=debug
   ```

2. Aprire log4j.properties e verificare che le voci di registro vengano visualizzate.

pdm_proctor_init - Avvio di proctor sui server secondari

Valido solo per l'ambiente UNIX.

Il comando pdm_proctor_init consente di avviare il proctor sui server secondari. Tutti i server secondari devono essere avviati prima di avviare i daemon dal server primario. Una volta che tutti i daemon sono stati arrestati dal server primario, immettere il comando pdm_halt sul server secondario per arrestare il proctor.

Nota: non utilizzare il comando pdm_proctor_init sul server primario.

Sintassi

Il comando presenta il seguente formato:

```
pdm_proctor_init
```

pdm_replace - Sostituzione di una tabella di database

Il comando pdm_replace consente di eliminare una tabella da un database di CA SDM e di sostituirla con una tabella ottenuta da un file temporaneo specificato tramite l'opzione -f. Dopo l'esecuzione del comando pdm_replace, la tabella contiene solo i dati del file di input. Creare una copia di backup della tabella prima di eseguire il comando pdm_replace.

Nota: come parte del processo, l'utilità pdm_replace per prima cosa arresta i daemon (UNIX) o i servizi (Windows).

Il comando pdm_replace accetta un file di testo come input, che corrisponde allo stesso formato file utilizzato dall'utilità pdm_userload. È possibile creare un file di input per l'utilità pdm_replace utilizzando l'utilità pdm_extract. Tuttavia, non è possibile utilizzare l'output generato dall'utilità pdm_backup come input per l'utilità pdm_replace.

Importante. Assicurare di assegnare al file di input un nome diverso dalla tabella che si sta tentando di sostituire. Ad esempio, se si sta sostituendo la tabella ca_contacts e il nome che si assegna al file di input è ca_contacts.dat, dopo aver eseguito il comando pdm_replace per puntare al file di input (ca_contacts.dat), al termine dell'esecuzione il file viene eliminato poiché ha lo stesso nome della tabella.

Restrictions

- È possibile eseguire pdm_replace solo sui server seguenti, a seconda della configurazione di CA SDM:
  - Convenzionale: server primario
  - Disponibilità avanzata: server in background

    Importante. Verificare di aver arrestato tutti i server applicazioni e i server di standby prima di eseguire il comando sul server in background.
- Soltanto un utente con privilegi o di livello root può eseguire il comando pdm_replace.
- Non eseguire il comando pdm_replace quando vi sono utenti connessi a CA SDM.

Sintassi

Il comando presenta il seguente formato:

```
pdm_replace [-v] -f nomefile
```

-v

Specifica la modalità dettagliata.

-f *filename*

Specifica un file ASCII con il formato seguente:

```
TABLE nome_tabella

nomecampo1 nomecampo2 . . . . nomecampoN

{ "value11", "value12", . . . "value1N" }

{ "value21", "value22", . . . "value2N" }

.

.

.

{ "valueN1", "valueN2", . . . "valueNN" }
```

Questo è lo stesso formato file utilizzato dal comando pdm_userload. È possibile creare un file di input per l'utilità pdm_replace utilizzando l'utilità pdm_extract. Tuttavia, non è possibile utilizzare l'output generato dall'utilità pdm_backup come input per l'utilità pdm_replace.

Ulteriori informazioni:

pdm_extract - Estrazione dei dati dal database (a pagina 1134)
pdm_userload - Aggiunta, aggiornamento ed eliminazione dei record del database (a pagina 1166)

Gestione dell'applicazione dei servizi Web RESTful di CA SDM - pdm_rest_util

CA SDM utilizza questa utilità automaticamente. Se lo si desidera è possibile eseguire questa utilità manualmente, ad esempio in seguito a un errore imprevisto. Questa utilità dei servizi Web REST esegue la distribuzione dell'applicazione Web dei servizi REST. Inoltre, esegue la distribuzione dell'applicazione REST sull'istanza Tomcat dedicata. Nella directory NX_ROOT\bin (pdm_rest_util.bat for Windows or ./pdm_rest_util.sh for UNIX) è disponibile un file batch che consente di richiamare l'utilità.

Questo comando presenta il seguente formato e opzioni:

```
pdm_rest_util –h | [-deploy] | [-undeploy]
```

-h

Consente di stampare la Guida della riga di comando.

-deploy

Consente di generare, compilare ed eseguire la distribuzione di tutti i factory Majic.

-undeploy

Consente di annullare la distribuzione dei servizi Web REST sul server locale.

Annullamento della distribuzione dell'applicazione dei servizi Web REST

È possibile annullare la distribuzione dell'applicazione dei servizi Web REST mediante l'utilità pdm_rest_util. Ad esempio, si desidera eseguire la manutenzione di CA SDM e annullare la distribuzione di REST durante questa operazione.

Procedere come descritto di seguito:

1. Aprire un prompt dei comandi.
2. Eseguire il comando riportato di seguito:

   ```
   pdm_rest_util -undeploy
   ```

   La distribuzione dell'applicazione dei servizi Web REST viene annullata.

Importante. Se la distribuzione dell'applicazione REST viene annullata utilizzando questa utilità, sarà possibile distribuire nuovamente REST al riavvio di CA SDM, in modo automatico. Si consiglia di utilizzare la configurazione di CA SDM per disabilitare REST.

pdm_restore - Ripristino di un database

Il comando pdm_restore arresta CA SDM, quindi elimina tutti i record da un database di CA SDM e li sostituisce con i record del file specificato tramite l'opzione -f. Dopo l'esecuzione del comando pdm_restore, il database di CA SDM conterrà solo i dati presenti nel file di input.

Il file di input deve essere creato con i comandi pdm_extract o pdm_backup oppure deve essere un file di formato compatibile con pdm_restore. Il comando pdm_backup è in grado di eseguire il backup di dati non tipici di database, mentre il comando pdm_restore supporta anche il ripristino di questi dati. Si consiglia di non utilizzare i comandi pdm_backup e pdm_restore se sono disponibili altri strumenti per il backup e il ripristino.

Nota: come parte del processo, l'utilità pdm_restore per prima cosa arresta i daemon (UNIX) o i servizi (Windows).

Sintassi

Il comando presenta il seguente formato:

```
pdm_restore [-d] [-g] [-n] [-w] [-v] –f nomefile
```

Restrictions

È possibile eseguire il comando pdm_restore solo su un server CA SDM. Soltanto un utente con privilegi o di livello root può eseguire il comando pdm_restore. Le restrizioni seguenti sono applicabili se si utilizza la configurazione con disponibilità avanzata:

- Se è in corso il ripristino del database, eseguire il comando pdm_restore solo sul server in background.
- Verificare di aver arrestato tutti i server (applicazioni, in background e di standby) prima di eseguire il comando pdm_restore.

Importante. Utilizzare il comando pdm_restore solo con il backup di un database completo creato con il comando pdm_backup, poiché il database corrente viene eliminato e sostituito dai dati presenti nel file di backup. Non eseguire il comando pdm_restore quando vi sono utenti connessi a CA SDM.

-d

Specifica che devono essere ripristinati solo i dati del database.

-g

Specifica che deve essere eseguito solo il ripristino dei dati non del database. Il ripristino riguarda solo i dati delle finestre (moduli) e altri elementi non di database.

-n

Specifica che viene ripristinato anche il file NX.env se si stanno ripristinando dati non di database. Per impostazione predefinita, il file NX.env non viene ripristinato. Si consiglia di non ripristinare il file NX.env a meno che non venga ripristinato sullo stesso server da cui era stata creata la copia di backup. Il ripristino di file NX.env non pertinenti può influire involontariamente sui database.

-w

Specifica che viene ripristinato anche il file web.cfg se si stanno ripristinando dati non di database. Per impostazione predefinita, il file web.cfg non viene ripristinato.

-v

Specifica la modalità dettagliata.

-f *filename*

Specifica un file di input che contiene un backup completo creato con il comando pdm_backup.

Importante: in UNIX, LIBPATH deve essere impostato prima di eseguire diverse utilità di CA SDM. Utilizzare *pdm_task* per impostare LIBPATH prima di eseguire un'utilità. Immettere ad esempio "pdm_task pdm_clean_attachments...".

Ulteriori informazioni:

pdm_userload - Aggiunta, aggiornamento ed eliminazione dei record del database (a pagina 1166)
pdm_backup - Scrittura di tabelle di database in file ASCII (a pagina 1124)
Ripristino del database (a pagina 519)

pdm_status - Stato dei daemon e dei processi

Il comando pdm_status mostra lo stato di tutti i daemon (UNIX) o processi (Windows) CA SDM presenti sul sistema dal quale viene eseguito.

L'output viene visualizzato in questo formato:

```
DAEMON                          STATUS      HOST       PID   SLUMP CONNECT TIME
-------------------------------------------------------------------------------
Agent anthill                   Running     anthill    455   Tue Feb 17 17:55:12
Ddict_rd              (ddictrd) Completed   anthill
Data Dictionary    (ddictbuild) Completed   anthill
...
User Validation       (boplgin) Running     anthill    456   Tue Feb 17 17:55:21
```

Sintassi

Il comando presenta il seguente formato:

```
pdm_status
```

pdm_task - Impostazione delle variabili di ambiente

Valido solo per l'ambiente UNIX.

Il comando pdm_task consente di impostare le variabili di ambiente per i comandi che non prevedono il wrapper. Ad esempio, il comando pdm_task deve precedere il comando report sulla stessa riga di comando **solo** se il comando viene richiamato tramite uno script oppure dalla riga di comando. Se si esegue il comando report da un menu, non è necessario includere il comando pdm_task poiché tutte le variabili di ambiente vengono impostate dall'applicazione.

Nota: non è possibile generare rapporti dalla riga di comando di un client.

Sintassi

Il comando presenta il seguente formato:

pdm_task *comando*

comando

Specifica un comando che non prevede un wrapper e, pertanto, non è in grado di impostare automaticamente le variabili di ambiente. Per ulteriori informazioni sull'esecuzione di pdm_task con un comando, consultare la sintassi del comando report--Generazione dei report (a pagina 1173).

Interfaccia riga di comando di Text API - pdm_text_cmd

Utilizzare il comando pdm_text_cmd per l'API di testo per creare e aggiornare diversi oggetti, quali Richieste, Ordini di cambiamento, Issue asset e contatti.

Importante. Non è possibile utilizzare le virgolette singole o doppie come parametro dei comandi pdm_text_nxd o bop_cmd.

Sintassi

Il comando presenta il seguente formato:

pdm_text_cmd –t *tabella* {-u *da_idutente* –p *da_idpersistente*} [-o *operazione* [-f *file_input*] [-T *timeout*] [-h]

-t *table*

(Obbligatorio) Specifica la tabella da elaborare. Il valore di *tabella* può essere uno dei seguenti (nessuna distinzione tra maiuscole e minuscole):

- Asset
- Contatto
- Cambiamento
- Issue
- Richiesta

Nota: vedere la sezione [OPTIONS] del file text_api.cfg per un elenco completo dei nomi di tabella validi.

-u *da_idutente* **| -p da_***idpersistente*

(1 opzione obbligatoria) Identifica il contatto per l'operazione:

-u ***da_idutente***

Identifica il contatto utilizzando il valore ID utente.

-p ***da_idpersistente***

Identifica il contatto utilizzando l'ID oggetto univoco del record del contatto. *da_idpersistente* deve avere formato **cnt:***xxxx. xxxx* è l'ID persistente dell'oggetto.

Nota: il valore specificato con questa opzione viene aggiunto in coda all'input del comando pdm_text_cmd, utilizzando la parola chiave appropriata, %FROM_USERID o %FROM_PERSID.

-o *operazione*

Specifica l'operazione da eseguire. Il valore di *operazione* può essere uno dei seguenti (nessuna distinzione tra maiuscole e minuscole):

- NEW—Crea un nuovo oggetto. Si tratta del valore predefinito se non è specificata alcuna operazione.
- UPDATE | UPD—Crea un oggetto se l'oggetto non viene trovato o aggiorna un oggetto esistente.
- UPDATE_ONLY | UPDO—Aggiorna l'oggetto se trovato, altrimenti non viene eseguita alcuna operazione.

Sia UPDATE che UPDATE_ONLY richiedono la parola chiave %SEARCH nell'input del comando. Ad ogni esecuzione del comando pdm_text_cmd è possibile specificare una sola operazione.

-f *file_input*

Specifica il percorso completo del file da elaborare. Si tratta di un file di testo contenente comandi validi dell'interfaccia API testo. Se si omette questo parametro, vengono utilizzati i comandi da STDIN. L'interfaccia API testo utilizza il seguente formato di base per l'input:

```
%parola_chiave=valore
```

È possibile utilizzare più comandi nell'input, separando la richiesta di comando con almeno cinque segni di percentuale (%%%%%).

Nota: per ulteriori informazioni sulle parole chiave valide e sulla formattazione dell'input per l'interfaccia API testo, vedere il file text_api.cfg.

-T *timeout*

Specifica il numero di secondi di attesa della risposta dal server trascorsi i quali si verifica il timeout. Il valore predefinito è 30 secondi.

Nota: pdm_text_cmd mostra le risposte in formato testo ricevute dall'interfaccia API testo, che includono messaggi di operazione riuscita o di errore, e il testo originale inviato utilizzando l'interfaccia API per l'elaborazione. pdm_text_cmd restituisce 0 (zero) se il comando viene eseguito correttamente senza avvisi o errori e 1 (uno) se viene eseguito correttamente ma con avvisi. Qualsiasi altro valore restituito indica che si è verificato un errore.

Importante: in UNIX, LIBPATH deve essere impostato prima di eseguire diverse utilità di CA SDM. Utilizzare *pdm_task* per impostare LIBPATH prima di eseguire un'utilità. Immettere ad esempio "pdm_task pdm_clean_attachments...".

Nota: per l'immissione dei parametri dal prompt dei comandi, utilizzare Ctrl+Z in Windows e Ctrl+D in POSIX.

Ulteriori informazioni:

Utilizzo dell'API testo (a pagina 553)

Esempi di input

Il comando pdm_text_cmd avvia l'interfaccia della riga di comando di Text API che consente di creare e aggiornare diversi oggetti, quali Richieste, Ordini di cambiamento, Issue, asset e contatti.

Esempio: uso di un file di input per creare una Issue

Il seguente esempio spiega come usare il file di input pdm_text_cmd per creare una Issue:

```
%DESCRIPTION=Testo di prova.
%PRIORITY=3
```

Per elaborare il file, se il percorso completo fosse c:\input.txt, il comando da immettere sarebbe:

```
pdm_text_cmd -t Issue –u user01 -f c:\input.txt
```

Esempio: uso di un file di input per aggiornare una Issue

L'esempio seguente mostra un file di input per assegnare alla Issue 123 la priorità 2:

```
%SEARCH=ISSUE_ID
%ISSUE_ID=123
%PRIORITY=2
```

Per elaborare il file, se il percorso completo fosse c:\input.txt, il comando da immettere sarebbe:

```
pdm_text_cmd -t Issue -o UPDATE_ONLY –u user01 -f c:\update.txt
```

Esempio: uso di un file di input per creare più richieste

L'esempio seguente mostra la creazione di più richieste in un unico file di input. Questo comando è utile per la creazione di dati di prova su un sistema di prova.

```
%DESCRIPTION=Prova personale 1.
%PRIORITY=3
%%%%%
%DESCRIPTION=Prova personale 2.
%PRIORITY=2
%%%%%
%DESCRIPTION=Prova personale 3.
%PRIORITY=Nessuna
```

Per elaborare il file, se il percorso completo fosse c:\input.txt, il comando da immettere sarebbe:

```
pdm_text_cmd -t Request –u user01-f c:\testdata.txt
```

pdm_uconv - Conversione di set di caratteri in UTF-8

L'utilità pdm_uconv assiste l'utente nella conversione dei dati da rilasci precedenti di CA SDM o integrazioni con altri prodotti CA Technologies. L'uso più comune di questa utilità consiste nella conversione da un set di caratteri locale a UTF-8 e da UTF-8 a un set di caratteri locale.

Sintassi

Il comando presenta il seguente formato:

```
pdm_uconv -h [-V] [-s] [-v] [-l | --list-code
| --default-code | -L] [--cannon] [-x] [--to-callback | -c] [--from-callback | -i]
[--fallback | --no-fallback] [-b] [-f] [--t] [--add-signature] [--remove-signature]
[-o] [file ...]
```

-h

Apre l'argomento della Guida .

-V

Stampa la versione del programma.

-s

Utilizza operazioni invisibili e sopprime i messaggi.

-v

Mostra le informazioni sull'avanzamento dell'utilità.

-l

Elenca tutte le codifiche disponibili. Sono validi i seguenti valori:

--list-code

Elenca solo le codifiche fornite.

--default-code

Elenca solo le codifiche predefinite.

-L

Elenca tutti i traslitteratori disponibili.

--cannon

Stampa l'elenco in formato cnvrtrs.txt(5).

-x

Esegue l'avanzamento attraverso la traslitterazione.

--to-callback *callback*

Utilizza il callback sulla codifica di destinazione.

-c

Omette dall'output caratteri non validi.

--from-callback *callback*

Utilizza il callback sulla codifica originale.

-i

Ignora sequenze non valide nell'immissione.

--callback *callback*

Utilizza il callback su entrambi gli encoding.s.

-b

Specifica le dimensioni del blocco.

Predefinito: 4096

--fallback

Utilizza la mappatura di fallback.

--no-fallback

Non utilizza la mappatura di fallback.

-f

Imposta la codifica originale.

-t

Imposta la codifica di destinazione.

--add-signature

Aggiunge il carattere della firma Unicode U+FEFF (BOM).

--remove-signature

Rimuove il carattere della firma Unicode U+FEFF (BOM).

-o

Scrive l'output su file.

Esempi:

Da set di caratteri locale a UTF-8

pdm_uconv -t utf-8 inputfile.txt > outputfile.txt

Da set di caratteri specifico (iso-2022-jp) a UTF-8

pdm_uconv -f iso-2022-jp -t utf-8 inputfile.txt > outputfile.txt

Da UTF-8 a set di caratteri locale

pdm_uconv -f utf-8 inputfile.txt > outputfile.txt

Da UTF-8 a set di caratteri specifico

pdm_uconv -f utf-8 -t iso-2022-jp inputfile.txt > outputfile.txt

L'utilità pdm_uconv dispone dei seguenti callback validi:

- substitute
- skip
- arresto
- escape
- escape-icu
- escape-java
- escape-c
- escape-xml
- escape-xml-hex
- escape-xml-dec
- escape-unicode

pdm_userload - Aggiunta, aggiornamento ed eliminazione dei record del database

L'utilità pdm_userload consente di aggiornare il database di CA SDM utilizzando un file di input specificato dall'utente.

Importante. Si consiglia di eseguire sempre il backup del database prima di utilizzare il comando pdm_userload.

Ogni volta che i ticket vengono caricati (ad esempio, Richieste o Issue), il numero di ticket deve includere un prefisso o un suffisso univoco nella stringa. CA SDM interpreta questo numero come stringa di caratteri e non come numero sequenziale. Pertanto, non viene assicurata l'assegnazione di un numero univoco ai ticket caricati. Tuttavia, se si assegna un prefisso o un suffisso univoco utilizzando Awk o un altro programma di elaborazione testi, è possibile caricare i ticket con la sicurezza che CA SDM non sovrascriva i ticket già esistenti.

Sintassi

Il comando presenta il seguente formato:

```
pdm_userload [-a] [-c] [-h] [-r] [-v] [-u] [-m] –f nomefile
```

Formato file di input

Il formato degli elementi del file di input è il seguente:

```
TABLE nome_tabella

nomecampo1 nomecampo2 . . . . nomecampoN

{ "value11", "value12", . . . "value1N" }

{ "value21", "value22", . . . "value2N" }

.

.

.

{ "valueN1", "valueN2", . . . "valueNN" }
```

table_name è il nome della tabella da caricare, come specificato nel file dello schema di database CA SDM, che si trova in $NX_ROOT/site/schema.sch (UNIX) oppure in *directory di installazione*\site\schema.sch (Windows), dove $NX_ROOT oppure *directory di installazione* è la directory in cui è installato CA SDM.

-f filename

Specifica il file di input in formato ASCII.

-a

Aggiorna tutti i record esistenti, senza tener conto se più di un record esistente corrisponde a un singolo record di input. Senza questa opzione, i record di input che corrispondono a più di un record esistente vengono rifiutati.

Importante. Utilizzare questa opzione con attenzione.

-c

Controlla il file di input con il database e segnala gli aggiornamenti necessari, ma non applica gli aggiornamenti.

-r

Rimuove i record dal database che corrispondono ai record di input. È possibile utilizzare l'opzione -a con l'opzione -r.

Nota: si consiglia di creare una copia di backup del database prima di eseguire il comando pdm_userload con questa opzione. Una volta rimossi i vecchi record dal database, per recuperare i record eliminati è necessario ripristinare il database di CA SDM con questa copia di backup.

-v

Specifica la modalità dettagliata.

-u

Aggiorna i record esistenti, ma non inserisce nuovi record nel database.

-m

Indica un aggiornamento di massa. Specificare questo parametro quando si deve aggiungere o eliminare un numero elevato di record. Questa opzione sopprime tutte le notifiche ai client relative agli aggiornamenti e invia un messaggio che indica di aggiornare la cache di una tabella quando il comando pdm_userload termina di elaborarla.

-x

Utilizza formati di input numerici sensibili alle impostazioni internazionali.

-t

Specifica nome o UUID del titolare a cui associare tutti i dati caricati con il titolare specificato. Questo argomento è valido solo quando è installata l'opzione multi-tenancy.

Pdm_userload supporta nuovi argomenti per l'istruzione TABLE, ovvero "Truncate" e "NoNewID". Questi argomenti sono specificati in un'opzione con parentesi opzionale dopo il nome della tabella. Ad esempio:

```
TABLE Call_Req (TRUNCATE, NONEWID)
```

Tronca

Implica l'esecuzione da parte di pdm_userload del comando TRUNCATE specifico del database per la tabella prima di caricare qualsiasi dato. In aggiunta, impone alla logica pdm_userload di utilizzare una logica di solo inserimento indipendentemente dagli argomenti della riga di comando, poiché tutti i record sono nuovi.

NoNewID

Implica l'uso del valore ID da parte di pdm_userload dal proprio file di controllo dell'immissione per le nuove righe nella tabella, piuttosto che generare un nuovo ID per i dati inseriti (la logica predefinita dell'opzione pdm_userload -i).

Restrictions

È possibile eseguire il comando pdm_userload mentre CA SDM è attivo, tuttavia le prestazioni potrebbero risentirne in modo significativo. Si consiglia di eseguire il comando pdm_userload quando nessun utente sta utilizzando CA SDM.

Ulteriori informazioni:

pdm_replace - Sostituzione di una tabella di database (a pagina 1154)
pdm_backup - Scrittura di tabelle di database in file ASCII (a pagina 1124)
pdm_restore - Ripristino di un database (a pagina 1157)

pdm_webstat - Statistiche sull'uso del Web

Utilizzare il comando pdm_webstat per ottenere le statistiche sulla sessione e sull'utente CA SDM per uno o più processi del motore Web. Il comando pdm_webstat mostra le sessioni cumulative, il numero massimo di sessioni soddisfatte contemporaneamente e le sessioni attive. Fornisce anche informazioni sui singoli utenti.

Sintassi

Il comando presenta il seguente formato:

```
pdm_webstat [-r] [-d | -D] [-i] [-t timeout] [-p motore_Web] [-n] [-h]
```

-r

Specifica la modalità di testo non elaborato, senza titoli e altra formattazione. Nell'output di un singolo processo del motore Web non ci sono interruzioni di riga. Tuttavia, l'output di ciascun processo del motore Web inizia sempre su una nuova riga.

La modalità di testo non elaborato visualizza i dati esattamente nello stesso ordine dell'output del comando pdm_webstat senza l'opzione -r. La modalità di testo non elaborato è utile quando si desidera utilizzare i dati risultanti in un foglio di lavoro o in un altro tipo di rapporto. Ad esempio, la sintassi seguente:

```
pdm_webstat -r
```

mostra l'output seguente:

```
10/11/2005 10:31:49 web:local:0 12 4 2
10/11/2005 10:31:49 web:local:1 9 2 2
```

-d

Specifica l'output dettagliato che visualizza le sessioni utente. L'opzione -d elenca tutte le sessioni correnti nel formato *ID_utente@indirizzo_IP*. Se una sessione viene visualizzata senza un ID utente, solitamente significa che nessun utente ha ancora utilizzato la sessione per l'accesso. Ad esempio, la sintassi seguente:

```
pdm_webstat -d
```

mostra l'output seguente:

```
PDM_Webstat: Invoked at 11/10/05 10:27:31
=========================================
Report from Webengine: web:local:0
=========================================
Cumulative sessions so far = 12
Most sessions at a time    = 4
Currently active sessions  = 2
  @192.168.1.16
  usery@192.168.1.20
=========================================
Report from Webengine: web:local:1
=========================================
Cumulative sessions so far = 7
Most sessions at a time    = 2
Currently active sessions  = 2
  SrvcPlus@192.168.1.14
  userx@192.168.1.8
```

-D

Genera output più dettagliato per motivi di debug. Questa opzione deve essere utilizzata solo se richiesto specificatamente dal Supporto tecnico di Computer Associates. Aggiunge informazioni interne su ciascuna sessione al normale output dettagliato. Ad esempio, la sintassi seguente:

```
pdm_webstat -D
```

mostra l'output seguente:

```
PDM_Webstat: Invoked at 11/10/07 10:28:10
==========================================
Report from Webengine: web:local:0
==========================================
Cumulative sessions so far = 12
Most sessions at a time    = 4
Currently active sessions  = 2
  @192.168.1.16           SessionStat   1
  userx@192.168.1.20      SessionStat   5
==========================================
Report from Webengine: web:local:1
==========================================
Cumulative sessions so far = 7
Most sessions at a time    = 2
Currently active sessions  = 2
  SrvcPlus@192.168.1.14   SessionStat   7
  userx@192.168.1.8       SessionStat  13
```

-i

Specifica l'intervallo in secondi di generazione dei report. Quando si specifica l'argomento -i, il comando pdm_webstat rimane sempre in esecuzione. Il comando pdm_webstat genera il report come output nel formato richiesto da altri argomenti, rimane in attesa per l'intervallo di tempo specificato, quindi genera nuovamente il report come output. Con l'argomento –i, l'esecuzione del comando pdm_webstat termina solo quando viene richiesto in modo esplicito, solitamente con la combinazioni di tasti Ctrl+C. Ad esempio, la sintassi seguente:

```
pdm_webstat –i 5 –p web:local –r
```

mostra l'output seguente:

```
21/09/07 16:27:25 web:local 14 10 6
21/09/07 16:27:30 web:local 17 10 9
21/09/07 16:27:35 web:local 18 10 10
21/09/07 16:27:41 web:local 21 13 13
```

-t timeout

Specifica il valore di timeout in secondi. Con questo parametro, il comando pdm_webstat attende la risposta per il numero di secondi specificato. Se la risposta non arriva entro questo intervallo di tempo, il comando termina. Il valore predefinito è 30 secondi.

-p motore_Web

Specifica il nome del processo del motore Web per cui si desidera generare il report. Per impostazione predefinita, viene generato un rapporto per tutti i processi del motore Web. Il nome del processo (chiamato anche slump-nome) è lo stesso nome riportato nell'output del comando slstat e inizia sempre con "web:".

-n

Sopprime le normali voci di registro per ciascun motore Web per il quale viene generato un report. Per impostazione predefinita, viene creata una voce di registro con informazioni riepilogative su ciascun processo del motore Web.

Nota: per impostazione predefinita, se non si specificano i parametri, il comando pdm_webstat visualizza dati di riepilogo per tutti i processi in esecuzione.

Il comando pdm_webstat restituisce zero se l'esecuzione riesce correttamente oppure un valore diverso da zero se si verificano errori (ad esempio, una condizione di timeout oppure nessun processo del motore Web attivo).

Esempio: output del comando pdm_webstat se non si specificano parametri

L'esempio seguente mostra l'output del comando pdm_webstat nel caso in cui venga eseguito senza specificare parametri:

```
PDM_Webstat: Invoked at 11/10/07 10:26:42
=========================================
Report from Webengine: web:local:0
=========================================
Cumulative sessions so far = 12
Most sessions at a time    = 4
Currently active sessions  = 2
=========================================
Report from Webengine: web:local:1
=========================================
Cumulative sessions so far = 7
Most sessions at a time    = 2
Currently active sessions  = 2
```

Importante: in UNIX, LIBPATH deve essere impostato prima di eseguire diverse utilità di CA SDM. Utilizzare *pdm_task* per impostare LIBPATH prima di eseguire un'utilità. Immettere ad esempio "pdm_task pdm_clean_attachments...".

report - Generazione dei rapporti

Valido solo per l'ambiente UNIX.

Il comando report consente di generare un rapporto dalla riga di comando del server. Per eseguire il comando report dalla riga di comando oppure in uno script, è necessario includere il comando pdm_task. Il comando pdm_task consente di impostare le variabili di ambiente per i comandi che non prevedono un wrapper. Immettere pdm_task con il comando report nella stessa riga di comando *solo* quando il report viene invocato tramite uno script o la riga di comando. Se si esegue il comando report da un menu, non è necessario includere il comando pdm_task poiché tutte le variabili di ambiente vengono impostate dall'applicazione.

Sintassi

Il comando presenta il seguente formato:

```
pdm_task report [-h] [-e] [-f] [-F stringa] [-p lunghezza_pagina] nomefile
[argomenti_riga_comando]
```

-e

Esegue l'eco dello script compilato (per motivi di debug).

-f

Applica l'avanzamento modulo tra le pagine.

-F ffstring

Imposta la stringa di avanzamento modulo opzionale.

-p pagelength

Imposta la lunghezza della pagina. La lunghezza della pagina predefinita è 66.

filename

Modello del report. Se non si esegue il comando report dalla directory in cui si trova il file modello, includere il percorso completo. Il comando invia l'output come output standard (stdout).

command line arguments

Specifica i parametri ricevuti dal modello del rapporto. Se il rapporto prevede l'accettazione degli argomenti della riga di comando, è necessario un argomento per ogni parametro nel modello di rapporto. Se l'argomento è vuoto, immettere una stringa Null.

Ad esempio, il comando seguente fornisce gli argomenti della riga di comando Smith, Jane e L. Il modello di report richiede questi tre parametri per generare il report relativo ai contatti interessati.

Ad esempio, immettere:

```
pdm_task report /opt/CAisd/samples/sdk/reports/affected.rpt
```

Nell'esempio successivo, Jane Smith non ha l'iniziale del secondo nome:

```
pdm_task report /opt/CAisd/samples/sdk/reports/affected.rpt Smith Jane "
```

rpt_srv - Generazione dei rapporti

Valido solo per Windows

Il comando report consente di generare un rapporto dalla riga di comando del server. Per eseguire il comando report dalla riga di comando oppure in uno script, è necessario includere il comando pdm_task. Il comando pdm_task consente di impostare le variabili di ambiente per i comandi che non prevedono un wrapper. Immettere pdm_task con il comando report nella stessa riga di comando solo quando il report viene invocato tramite uno script o la riga di comando. Se si esegue il comando report da un menu, non è necessario includere il comando pdm_task poiché tutte le variabili di ambiente vengono impostate dall'applicazione.

Sintassi

Il comando presenta il seguente formato:

```
rpt_srv –m [-h] [-e] [-f] [-F ffstring] [-p pagelength] [-C] [-B] filename
[argomenti della riga di comando]
```

-m

Indica che il rapporto viene generato manualmente dalla riga di comando.

-e

Esegue l'eco dello script compilato (per motivi di debug).

-f

Applica l'avanzamento modulo tra le pagine.

-F *ffstring*

Imposta la stringa di avanzamento modulo opzionale.

-p *pagelength*

Imposta la lunghezza della pagina. La lunghezza della pagina predefinita è 66.

-C

Modifica la codifica da UTF-8 a un altro set di caratteri. L'output predefinito è UTF-8.

Esempio: per convertire l'output in JIS, è necessario eseguire "-C iso-2022-jp"

Esempio: per la codifica nel set di caratteri nativo del sistema operativo, usare "DEFAULT" o "NATIVE".

-B

Sopprime il Byte Order Mark se è impostata la variabile NX_ADD_UTF8_BYTE_ORDER_MARK.

L'opzione NX_ADD_UTF8_BYTE_ORDER_MARK è una firma in un file. Consente editor che supportano UTF-8 per gestire l'integrità UTF-8 del file.

Nota: questo è necessario solo per dati non-ASCII. Se non viene installato, il comportamento predefinito omette il Byte Order Mark (BOM). Se installato, impostarlo su "1" o "Sì".

filename

Specifica il modello del report. Se non si esegue il comando report dalla directory in cui si trova il file modello, includere il percorso completo. Il comando invia l'output come output standard (stdout).

command line arguments

Specifica i parametri ricevuti dal modello del rapporto. Se il rapporto prevede l'accettazione degli argomenti della riga di comando, è necessario un argomento per ogni parametro nel modello di rapporto. Se l'argomento è vuoto, immettere una stringa Null.

Ad esempio, il comando seguente fornisce gli argomenti della riga di comando Smith, Jane e L. Il modello di report richiede questi tre parametri per generare il report relativo ai contatti interessati.

Ad esempio, immettere il comando riportato di seguito:

```
rpt_srv –m c:\reports\affected.rpt Smith Jane L
```

Nell'esempio successivo, Jane Smith non ha l'iniziale del secondo nome:

```
rpt_srv –m c:\reports\affected.rpt Smith Jane "
```

uniconv - Avvio del daemon convertitore eventi CA NSM UNIX

Valido solo per l'ambiente UNIX.

Se CA SDM è integrato con CA NSM, è possibile usare il comando uniconv per inviare i dati relativi agli eventi generici ai daemon dei filtri in CA SDM. Il comando uniconv viene usato in un messaggio azione in Gestione eventi CA NSM.

Sintassi

Il comando presenta il seguente formato:

```
uniconv –h &opnode –e &’text’ [-n &

nodeid] [-u &userid] [-d &datem] [-t &’

time’]
```

Restrictions

Il comando uniconv deve essere eseguito dalla directory $NX_ROOT/bin in UNIX. Per utilizzare questa utilità, è necessario che il sito sia integrato con CA NSM.

-h &opnode

Specifica il nome del nodo del computer su cui è in esecuzione il comando uniconv (obbligatorio).

-e &'text'

Specifica il testo completo del messaggio (obbligatorio).

-n &nodeid

Specifica il nome del nodo da cui ha avuto origine il messaggio (obbligatorio).

-u &userid

Specifica l'ID accesso della persona che ha generato il messaggio.

-d &datem

Specifica la data di sistema nel formato *gg/mm/aa*.

-t &'time'

Specifica l'ora di sistema.

Utilità pdm_mail - Invio di informazioni di posta elettronica

L'utilità pdm_mail viene utilizzata nelle notifiche per inviare posta elettronica mediante l'invio di informazioni di posta elettronica al processo pdm_mail_nxd. L'utilità pdm_mail può anche essere utilizzata per i comandi, ma non per entrambi. Se non vengono utilizzati parametri, è attivo il comportamento predefinito di utilizzo della variabile NX_NTF_xxxx per passare parametri.

Per la posta elettronica l'utilità viene richiamata nel modo seguente:

```
pdm_mail [-i [-s subject] [-e email_address] [-q]] [-p] [-M] [-F] [-T] [-B] [-H] [-N]
[-R] [-h]
```

-i

Utilizza STDIN invece delle variabili NTF. I seguenti parametri vengono utilizzati solo per il comportamento della posta elettronica STDIN:

-e

Specifica l'indirizzo di posta elettronica (per il destinatario).

-s

Specifica l'oggetto del messaggio di posta elettronica.

-q

Disattiva la visualizzazione del prompt per STDIN.

-p

Utilizza la logica del cercapersone. Questa opzione include l'utilizzo dell'indirizzo di posta elettronica del cercapersone anziché del normale indirizzo di posta elettronica. Viene utilizzata solo la versione di testo semplice (e non quella HTML).

-M

Utilizza solo testo semplice (e non MIME) nel corpo.

-F

Specifica l'indirizzo di provenienza del messaggio di posta elettronica.

-T

Specifica l'indirizzo di risposta del messaggio di posta elettronica.

-B

Specifica il set di caratteri del corpo. Ciò può essere utile per i cercapersone che non supportano il formato UTF-8.

-H

Specifica il set di caratteri del corpo. Ciò può essere utile per i cercapersone che non supportano il formato UTF-8.

-N

Specifica l'opzione Notifica sullo stato del recapito (DSN).

-R

Specifica l'opzione Restituzione Notifica sullo stato del recapito (DSN).

-h

Visualizza la Guida in linea dell'utilità.

Per i comandi l'utilità viene richiamata nel modo seguente:

Comando per il server di posta elettronica

```
pdm_mail -c option [parametro]
```

Comando per il sistema di ricezione

```
pdm_mail -x option [parametro]
```

check_interval

(solo -x) Modifica l'intervallo di controllo della posta elettronica in un valore specificato (in secondi).

report_interval

Modifica l'intervallo report in un valore specificato (in secondi).

report_now

Impone la creazione di un report per i registri. Il contatore non viene reimpostato.

send_q

(solo -c) Invia la coda di posta elettronica locale al server di posta elettronica remoto.

trace

Attiva o disattiva la funzione di traccia.

Importante: in UNIX, LIBPATH deve essere impostato prima di eseguire diverse utilità di CA SDM. Utilizzare *pdm_task* per impostare LIBPATH prima di eseguire un'utilità. Immettere ad esempio "pdm_task pdm_clean_attachments...".

Utilità pdm_server_control--Identificazione dei server

I comandi pdm_server_utility identificano il server come server in background o di standby in una configurazione con disponibilità avanzata.

Eseguire il seguente comando dal prompt dei comandi:

```
pdm_server_control -h | -b | -q interval [-s server_name] | -t | -c [-server_name]
```

-h

Visualizza la pagina della Guida.

-b

Indica a un server di standby locale di diventare il server in background. Il server di standby deve essere in esecuzione. Se il server non è in esecuzione, viene avviato ma viene eseguito alcun failover. Per avviare un failover, eseguire di nuovo il comando.

-q interval [-s server_name]

Notifica a un server applicazioni locale o remoto di rimanere inattivo in un intervallo di tempo specificato. Questo intervallo è il numero di secondi che trascorrono prima dell'arresto del server. Utilizzando questa opzione senza un server_name, il server locale riceve una notifica di disattivazione. Non è possibile utilizzare questa opzione per un server in background o di standby.

-t

Visualizza il tipo di questo server con disponibilità avanzata di CA SDM.

-c [-s server_name]

Invia una notifica a un server applicazioni locale o remoto affinché elimini la richiesta precedente di disattivazione.

Appendice B: Descrizione dei campi delle visualizzazioni

Questa sezione contiene i seguenti argomenti:

Descrizione dei campi delle visualizzazioni (a pagina 1182)
View_Act_Log (a pagina 1182)
View_Audit_Assignee (a pagina 1183)
View_Audit_Group (a pagina 1184)
View_Audit_Priority (a pagina 1185)
View_Audit_Status (a pagina 1185)
View_Change_Act_Log (a pagina 1186)
View_Change (a pagina 1187)
View_Change_to_Assets (a pagina 1192)
View_Change_to_Change_Act_Log (a pagina 1193)
View_Change_to_Change_WF (a pagina 1194)
View_Change_to_Properties (a pagina 1196)
View_Contact_Full (a pagina 1197)
View_Contact_to_Environment (a pagina 1200)
View_Group (a pagina 1200)
View_Group_to_Contact (a pagina 1201)
View_Issue (a pagina 1202)
View_Issue_Act_Log (a pagina 1206)
View_Issue_to_Assets (a pagina 1207)
View_Issue_to_Issue_Act_Log (a pagina 1208)
View_Change_to_Request (a pagina 1209)
View_Issue_to_Issue_WF (a pagina 1212)
View_Issue_to_Properties (a pagina 1214)
View_Request (a pagina 1215)
View_Request_to_Act_Log (a pagina 1221)
View_Request_to_Properties (a pagina 1221)

Descrizione dei campi delle visualizzazioni

È possibile utilizzare le informazioni di descrizione dei campi nelle visualizzazioni di base e avanzate fornite con CA SDM.

Le informazioni riportate nell'elenco seguente sono valide per la maggior parte delle tabelle.

- Per visualizzare i dati nelle visualizzazioni avanzate è necessario attivare il registro di audit disponibile in Amministrazione, Gestione opzioni, Registro di audit.

  Nota: per ulteriori informazioni sui registri di audit, consultare la *Guida in linea*.

- Il parametro pdmtime fa riferimento ai campi data/ora in formato GMT (il numero di secondi trascorsi dalla data 1/1/1970).
- I termini "Richiesta di cambiamento" e "Ordine di cambiamento" sono sinonimi.

Ulteriori informazioni:

Creazione di report in CA SDM (a pagina 915)

View_Act_Log

Di seguito è riportata la descrizione della visualizzazione di base della tabella act_log di una Richiesta. Questa visualizzazione include anche il tipo di attività e il nome completo dell'analista. La tabella act_log è stata unita alle tabelle act_type e ca_contact per fornire il tipo di attività effettivo di ciascuna voce del registro e l'analista che ha eseguito l'attività. I campi estratti dalle unioni che possono risultare utili si trovano alla fine dell'elenco.

Campo	**Commenti**
id	act_log.id: ID univoco del record della tabella act_log.
persid	act_log.persid: ID univoco del record della tabella act_log, preceduto dall'ID oggetto (alg per la tabella act_log) e dal segno due punti (:).
call_req_id	act_log.call_req_id: puntatore all'ID persistente richiesta chiamata a cui appartiene questa attività. act_log.call_req_id = call_req.persid.
last_mod_dt	act_log.last_mod_dt: data/ora dell'ultima modifica (pdmtime).
time_spent	act_log.time_spent: tempo trascorso per questa attività, memorizzato come numero totale di secondi. Ad esempio, 80 = 1 minuto e 20 secondi.
time_stamp	act_log.time_stamp: data/ora dell'attività modificabile dall'utente (pdmtime).
system_time	act_log.system_time: data/ora di creazione di record (pdmtime).

Campo	Commenti
analista	act_log.analyst: puntatore UUID all'UUID del contatto per indicare l'analista che ha eseguito l'attività. act_log.analyst = ca_contact.contact_uuid.
description	act_log.description: descrizione di testo dell'attività modificabile dall'utente.
action_desc	act_log.action_desc: descrizione dell'azione automatizzata non modificabile dall'utente.
tipo	act_log.type: puntatore di testo a un record nella tabella dei tipi attività. Ad esempio, act_log.type = act_type.code.
knowledge_session	act_log.knowledge_session: ID di una particolare sessione di un particolare utente.
knowledge_tool	act_log.knowledge_tool: indicatore dello strumento della conoscenza utilizzato per la ricerca, ad esempio: NLS_FAQ, EXPERT e così via.
interna	act_log.internal: flag numerico intero (1 o 0) che indica se la voce del registro è per solo uso interno oppure per tutti.
activity_type	act_type.symActivity: tipo di attività derivato da act_log.type = act_type.code.
analyst_lastname	View_Contact_Full.last_name: cognome dell'analista, derivante da act_log.analyst = ca_contact.contact_uuid.
analyst_firstname	View_Contact_Full.first_name: il nome dell'analista.
analyst_middlename	View_Contact_Full.middle_name: secondo nome dell'analista.

View_Audit_Assignee

Di seguito si descrive la visualizzazione avanzata del registro attività che prende in esame l'assegnatario. Questa visualizzazione mostra il tempo che intercorre tra i Cambiamenti di tipo assegnatario per ogni Richiesta (oppure Ordine di cambiamento). Se una Richiesta o un Ordine di cambiamento passa da un assegnatario specifico a nessun assegnatario e, successivamente, viene associata a un nuovo assegnatario, la visualizzazione non indicherà il tempo durante il quale la Richiesta o l'Ordine di cambiamento non è stato associato ad alcun assegnatario. Questa visualizzazione contiene i campi seguenti sia per le Richieste che per gli OrdinI di cambiamento. Il campo audobj_uniqueid può contenere più voci (Richieste o OrdinI di cambiamento).

Campo	Commenti
audobj_uniqueid	audit_log.audobj_uniqueid: ID univoco dell'oggetto registro di audit. Rappresenta chg.id (ID Ordine di cambiamento) o call_req.id (ID Richiesta).
from_val	audit_log.attr_after_val: il valore "modificato da" relativo all'assegnatario.

Campo	Commenti
to_val	audit_log.attr_after_val: il valore "modificato a" relativo all'assegnatario.
from_time	audit_log.attr_from_time: ora di inizio assegnazione dell'assegnatario (pdmtime).
to_time	audit_log.attr_from_time: ora di fine assegnazione dell'assegnatario (pdmtime).

View_Audit_Group

Di seguito si descrive la visualizzazione avanzata del registro attività. Tale visualizzazione tiene traccia del gruppo. Questa visualizzazione mostra il tempo che intercorre tra i cambiamenti di tipo gruppo per ogni Richiesta (oppure Ordine di cambiamento). Se una Richiesta (oppure un Ordine di cambiamento) passa da un gruppo specifico a nessun gruppo e quindi viene nuovamente associata a un particolare gruppo, in questa visualizzazione non viene riportato il tempo durante il quale la Richiesta (oppure l'Ordine di cambiamento) non era associata ad alcun gruppo. Questa visualizzazione contiene i campi seguenti sia per le Richieste che per gli Ordini di cambiamento. Il campo audobj_uniqueid può contenere più voci (Richieste o Ordini di cambiamento).

Campo	Commenti
audobj_uniqueid	audit_log.audobj_uniqueid: ID univoco dell'oggetto registro di audit. Rappresenta chg.id (ID Ordine di cambiamento) o call_req.id (ID Richiesta).
from_val	audit_log.attr_after_val: il valore "modificato da" relativo al gruppo.
to_val	audit_log.attr_after_val: il valore "modificato a" relativo al gruppo.
from_time	audit_log.attr_from_time: ora di inizio assegnazione del gruppo (pdmtime).
to_time	audit_log.attr_from_time: ora di fine assegnazione del gruppo (pdmtime).

View_Audit_Priority

Di seguito si descrive la visualizzazione avanzata del registro attività. Tale visualizzazione tiene traccia della priorità. Questa visualizzazione mostra il tempo che intercorre tra i Cambiamenti di tipo priorità per ogni Richiesta (oppure Ordine di cambiamento). Questa visualizzazione contiene i campi seguenti sia per le Richieste che per gli Ordini di cambiamento. Il campo audobj_uniqueid può contenere più voci (Richieste o Ordini di cambiamento).

Campo	Commenti
audobj_uniqueid	audit_log.audobj_uniqueid: ID univoco dell'oggetto di audit. Rappresenta un ID Richiesta (call_req.id) oppure un ID Ordine di cambiamento (chg.id).
from_val	audit_log.attr_after_val: il valore di priorità ‘modificato da’.
to_val	audit_log.attr_after_val: il valore di priorità ‘modificato a’.
from_time	audit_log.attr_from_time: ora di inizio di un particolare stato (pdmtime) relativo alla priorità.
to_time	audit_log.attr_from_time: ora di fine di un particolare stato (pdmtime) relativo alla priorità.

View_Audit_Status

Di seguito si descrive la visualizzazione avanzata del registro attività. Tale visualizzazione tiene traccia dello stato. Questa visualizzazione mostra il tempo che intercorre tra i cambiamenti di tipo stato per ogni richiesta (oppure Ordine di cambiamento). Questa visualizzazione contiene i campi seguenti sia per le Richieste che per gli Ordini di cambiamento. Il campo audobj_uniqueid può contenere più voci (Richieste o Ordini di cambiamento).

Campo	Commenti
audobj_uniqueid	audit_log.audobj_uniqueid: ID univoco dell'oggetto di audit. Rappresenta un call_req.id (ID Richiesta) oppure un chg.id (ID Ordine di cambiamento).
from_val	audit_log.attr_after_val: il valore di priorità ‘modificato da’.
to_val	audit_log.attr_after_val: il valore di priorità ‘modificato a’.
from_time	audit_log.attr_after_time: ora di inizio di un particolare stato (pdmtime) relativo allo stato.

Campo	Commenti
to_time	audit_log.attr_after_time: ora di fine di un particolare stato (pdmtime) relativo allo stato.

View_Change_Act_Log

Di seguito è riportata la descrizione della visualizzazione di base di tutti i registri delle attività correlate agli Ordini di cambiamento. Si tratta di una visualizzazione della tabella chgalg unita alle tabelle act_type e ca_contact per fornire dati più significativi, quali il tipo effettivo di attività e il nome completo dell'analista che ha eseguito l'attività.

Campo	Commenti
id	chgalg.id: identificatore unico per questo record nella tabella chgalg.
persid	chgalg.persid: identificatore unico per questo record nella tabella chgalg, preceduto dall'identificatore di oggetto (chgalg per chgalg) e due punti.
change_id	chgalg.change_id: puntatore all'ID dell'Ordine di cambiamento a cui appartiene l'attività. chgalg.change_id = chgalg.id
last_mod_dt	chgalg.last_mod_dt: l'ultima data/ora modificata (pdmtime).
time_spent	chgalg.time_spent: periodo trascorso per questa attività, memorizzato come numero totale di secondi. Ad esempio, 80 = 1 minuto e 20 secondi.
time_stamp	chgalg.time_stamp: data/ora di attività modificabile dall'utente (pdmtime).
system_time	chgalg.system_time: data/ora di creazione di record (pdmtime).
analista	chgalg.analyst: puntatore UUID all'UUID del contatto che indica l'analista che ha eseguito l'attività. chgalg.analyst = ca_contact.contact_uuid
description	chgalg.description: descrizione di testo di questa attività, la quale può essere modificata dall'utente.
action_desc	chgalg.action_desc: descrizione di testo dell'azione automatica, la quale non può essere modificata dall'utente.
tipo	chgalg.type: puntatore di testo a un record nella tabella di tipo attività. chgalg.type = act_type.code
interna	chgalg.internal: flag intero (1 o 0), che indica se questa voce di registro è visibile a tutti o è diretta al solo uso interno.

Campo	Commenti
knowledge_session	chgalg.knowledge_session: ID di una particolare sessione di un particolare utente.
knowledge_tool	chgalg.knowledge_tool: indicatore dello strumento della conoscenza utilizzato per la ricerca, ad esempio NLS_FAQ, EXPERT e così via.
analyst_lastname	View_Contact_Full.last_name: cognome dell'analista derivante da chgalg.analyst = ca_contact.contact_uuid.
analyst_firstname	View_Contact_Full.first_name: primo nome dell'analista.
analyst_middlename	View_Contact_Full.middle_name: secondo nome dell'analista.
activity_type	act_type.sym: tipo di attività a cui si fa riferimento tramite chgalg.type = act_type.code.

View_Change

Di seguito si riporta la visualizzazione di base per tutti gli Ordini di cambiamento che mostra informazioni quali lo stato, la priorità, la categoria, le organizzazioni, il nome completo dell'utente interessato, il nome completo del richiedente, il nome completo dell'assegnatario, il nome del gruppo, l'ID ecc. La tabella Richiesta di cambiamento (chg) è stata unita con altre tabelle per fornire dati più significativi sugli Ordini di cambiamento.

Campo	Commenti
id	chg.id: ID univoco del record della tabella chg.
persid	chg.persid: ID univoco del record della tabella chg, preceduto dall'ID dell'oggetto (chg per la tabella chg) e dal segno due punti (:).
chg_ref_num	chg.chg_ref_num: numero di riferimento dell'Ordine di cambiamento utilizzato dagli analisti e dai clienti per fare riferimento a un particolare Ordine di cambiamento.
description	chg.description: descrizione estesa di un Ordine di cambiamento come specificata da un analista o da un cliente.
status	chg.status: ID univoco dello stato di un Ordine di cambiamento, che costituisce il puntatore alla tabella chgstat: chg.status = chgstat.code.
active_flag	chg.active_flag: flag numerico che determina se il record di Cambiamento è attivo o non attivo (1 o 0).

Campo	Commenti
start_date	chg.start_date: data in cui la prima attività è passata allo stato In sospeso (pdmtime).
open_date	chg.open_date: data di creazione dell'Ordine di cambiamento (pdmtime).
last_mod_dt	chg.last_mod_dt: data dell'ultima modifica (pdmtime).
last_mod_by	chg.last_mod_by: puntatore all'UUID dell'ultimo contatto che ha modificato l'Ordine di cambiamento. chg.last_mod_by = ca_contact.contact_uuid.
close_date	chg.close_date: data in cui l'Ordine di cambiamento è stato impostato su Non attivo (pdmtime).
resolve_date	chg.resolve_date: data in cui l'Ordine di cambiamento è stato impostato su uno stato configurato per indicare che il Cambiamento è stato risolto (pdmtime).
rootcause	chg.rootcause: puntatore a un record nella tabella rootcause che indica la situazione da cui è derivato l'Ordine di cambiamento. chg.rootcause = rootcause.id
est_total_time	chg.est_total_time: tempo totale stimato (pdmtime) per il completamento del Cambiamento.
actual_total_time	chg.actual_total_time: tempo totale effettivo (pdmtime) per il completamento del Cambiamento.
log_agent	chg.log_agent: ID binario univoco relativo alla tabella ca_contact che indica la persona che ha creato il Cambiamento. chg.log_agent = ca_contact.contact_uuid
assignee	chg.assignee: puntatore all'UUID del contatto assegnato all'Ordine di cambiamento. chg.assignee = ca_contact.contact_uuid
organization	chg.organization: puntatore all'UUID dell'organizzazione interna, ovvero l'organizzazione alla quale appartiene l'Ordine di cambiamento. chg.organization = ca_organization.organization_uuid.
group_id	chg.group_id: puntatore all'UUID del contatto, che rappresenta il gruppo assegnato all'Ordine di cambiamento. chg.group_id = ca_contact.contact_uuid
affected_contact	chg.affected_contact: puntatore all'UUID del contatto, che rappresenta il contatto interessato dall'Ordine di cambiamento. chg.affected_contact = ca_contact.contact_uuid
requestor	chg.requrestor: puntatore all'UUID del contatto, che rappresenta l'utente che ha richiesto il Cambiamento. chg.requestor = ca_contact.contact_uuid

Campo	Commenti
category	chg.category: puntatore al codice della categoria di Cambiamento che consente di individuare la categoria di appartenenza del Cambiamento. chg.category = chgcat.code
priority	chg.priority: puntatore all'enumerazione di priorità, che rappresenta la priorità associata al Cambiamento. chg.priority = pri.enum
need_by	chg.need_by: data che indica quando l'utente finale interessato (affected_end_user) desidera che venga completato il Cambiamento (pdmtime).
est_comp_date	chg.est_comp_date: data stimata di completamento (pdmtime) dell'Ordine di cambiamento.
actual_comp_date	chg.actual_comp_date: data effettiva di completamento (pdmtime) dell'Ordine di cambiamento.
est_cost	chg.est_cost: costo stimato dell'Ordine di cambiamento.
actual_cost	chg.actual_cost: costo effettivo dell'implementazione dell'Ordine di cambiamento.
justification	chg.justification: campo di testo che consente al richiedente di specificare il motivo del Cambiamento.
backout_plan	chg.backout_plan: campo di testo che consente a un analista di specificare un piano alternativo per il Cambiamento
impact	chg.impact: puntatore a un record della tabella Impatto che indica l'ambito delle risorse interessate dal Cambiamento. chg.impact = impact.enum
parent	chg.parent: puntatore a un diverso ID di Richiesta di cambiamento che consente di creare una gerarchia di Ordini di cambiamento. chg.parent = chg.id
effort	chg.effort: campo di testo che spiega il piano di implementazione dell'Ordine di cambiamento.
support_lev	chg.support_lev: puntatore a un record di Service Desk che automatizza alcuni vincoli richiesti per il completamento del Cambiamento. chg.support_lev = srv_desc.code
template_name	chg.template_name: nome e puntatore di un modello di Ordine di cambiamento. chg.template_name = chg_template.template_name
sla_violation	chg.sla_violation: numero intero che indica il numero di violazioni SLA associate al Cambiamento.
predicted_sla_viol	chg.predicted_sla_viol: campo con tecnologia Neugent (r5.5).

Campo	Commenti
macro_predict_viol	chg.macro_predict_viol: campo con tecnologia Neugent (r5.5).
created_via	chg.created_via: puntatore a un record della tabella interface. Indica l'interfaccia utilizzata per creare l'Ordine di cambiamento. chg.created_via = interface.id
call_back_date	chg.call_back_date: campo di data/ora (pdmtime) che indica la data e l'ora in cui contattare il richiedente.
call_back_flag	chg.call_back_flag: indicatore booleano visualizzato dall'utente sotto forma di casella di controllo. Indica se inviare una notifica all'analista alla data specificata in chg.call_back_date.
string1	Campo di testo definibile dall'utente.
string2	Campo di testo definibile dall'utente.
string3	Campo di testo definibile dall'utente.
string4	Campo di testo definibile dall'utente.
string5	Campo di testo definibile dall'utente.
string6	Campo di testo definibile dall'utente.
service_date	chg.service_date: data/ora prevista (pdmtime) per l'esecuzione dell'Ordine di cambiamento da parte del vendor esterno.
service_num	chg.service_num: campo di testo in cui indicare il numero di ordine di acquisto o di assistenza del vendor esterno.
product	chg.product: puntatore a un record nella tabella Prodotto che indica il prodotto interessato dalla modifica. chg.product = product.id
actions	chg.actions: campo di testo esteso per la documentazione delle azioni.
type_of_contact	chg.type_of_contact: puntatore a un record nella tabella toc che indica la classificazione generale del punto di vista dell'utente finale (affected_end_user) interessato in merito all'Ordine di cambiamento. chg.type_of_contact = toc.id
reporting_method	chg.reporting_method: puntatore a un record della tabella repmeth che classifica la fonte dell'Ordine di cambiamento e viene selezionato dalla persona che crea l'Ordine di cambiamento. chg.reporting_method = repmeth.id
person_contacting	chg.person_contacting: puntatore a un record della tabella perscon che indica il ruolo dell'utente finale (affected_end_user) interessato o del richiedente. chg.person_contacting = perscon.id
status_name	chgstat.sym: descrizione dello stato visualizzata dall'utente. chg.status = chgstat.code

Campo	Commenti
priority_num	pri.sym: descrizione della priorità visualizzata dall'utente. chg.priority = pri.enum
category_name	chgcat.sym: nome della categoria di modifica visualizzato dall'utente. chg.category = chgcat.code
organization_name	ca_organization.org_name: nome di un'organizzazione visualizzato dall'utente. chg.organization = ca_organization.organization_uuid
affected_end_user_lastname	ca_contact.last_name: cognome dell'utente finale interessato. chg.affected_end_user = ca_contact.contact_uuid
affected_end_user_firstname	ca_contact.first_name: nome dell'utente finale interessato. chg.affected_end_user = ca_contact.contact_uuid
affected_end_user_middlename	ca_contact.middle_name: secondo nome dell'utente finale interessato. chg.affected_end_user = ca_contact.contact_uuid
requester_lastname	ca_contact.last_name: cognome del richiedente. chg.requestor = ca_contact.contact_uuid
requester_firstname	ca_contact.first_name: nome del richiedente. chg.requestor = ca_contact.contact_uuid
requester_middlename	ca_contact.middle_name: secondo nome del richiedente. chg.requestor = ca_contact.contact_uuid
business	ca_organization.org_name: nome dell'organizzazione del richiedente visualizzato dagli utenti. chg.requestor = ca_organization.organization_uuid
assignee_lastname	ca_contact.last_name: cognome dell'assegnatario. chg.assignee = ca_contact.contact_uuid
assignee_firstname	ca_contact.first_name: nome dell'assegnatario. chg.assignee = ca_contact.contact_uuid
assignee_middlename	ca_contact.middle_name: secondo nome dell'assegnatario. chg.assignee = ca_contact.contact_uuid
groupID	ca_contact.contact_uuid: rappresentazione binaria dell'ID interno utilizzato per il gruppo assegnato all'Ordine di cambiamento. chg.group_id = ca_contact.contact_uuid
group_name	ca_contact.last_name: nome del gruppo assegnato all'Ordine di cambiamento. chg.group = ca_contact.contact_uuid
service_type	srv_desc.sym: nome del tipo di servizio applicato all'Ordine di cambiamento. chg.support_lev = srv_desc.code

Campo	Commenti
impact_num	impact.sym: descrizione dell'impatto visualizzata dagli utenti. chg.impact = impact.enum
product_sym	product.sym: descrizione del prodotto visualizzata dagli utenti. chg.product = product.id
type_of_contact_sym	toc.sym: descrizione del tipo di contatto visualizzata dagli utenti. chg.type_of_contact = toc.id
rpting_method_sym	repmeth.sym: descrizione del metodo di reporting dal punto di vista dell'utente. chg.reporting_method = repmeth.id
person_contacting_sym	perscon.sym: descrizione della persona di contatto visualizzata dagli utenti. chg.person_contacting = perscon.id

View_Change_to_Assets

Il seguente elenco di campi offre una visualizzazione di base degli Ordini di cambiamento e dei relativi asset. La tabella chg è indirettamente unita alla tabella ca_owned_resource per ottenere un elenco degli asset di ciascun Ordine di cambiamento. È possibile che questa visualizzazione non includa tutti gli Ordini di cambiamento, in particolare gli Ordini a cui non sono associati asset.

Campo	Commenti
View_Change.*	Tutti i campi della visualizzazione View_Change sono stati definiti in precedenza in questo documento.
assetID	ca_owned_resource.own_resource_uuid - Campo binario che funziona come identificativo univoco interno, non modificabile, del record di un asset.
asset_serial_num	ca_owned_resource.serial_number - Numero di serie del record di un asset.
asset_class	ca_resource_class.name - Breve descrizione della classe di appartenenza dell'asset. ca_owned_resource.resource_class = ca_resource_class.id
asset_family	ca_resource_family.name - Famiglia di asset a cui appartiene l'asset. ca_owned_resource.resource_class = ca_resource_class.id e ca_resource_class.family_id = ca_resource_family.id
asset_name	ca_owned_resource.resource_name - Nome di rete con il quale è noto l'asset.

View_Change_to_Change_Act_Log

Di seguito è riportata la descrizione della visualizzazione di base di tutti gli Ordini di cambiamento e dei relativi registri delle attività. Questa visualizzazione è il risultato dell'unione della visualizzazione View_Change e della tabella chgalg e fornisce informazioni dettagliate sugli Ordini di cambiamento e sui relativi registri delle attività.

Campo	Commenti
View_Change.*	Visualizza tutti i campi della visualizzazione View_Change definiti in precedenza in questo documento.
chgalg_id	chgalg.id: identificatore unico per questo record nella tabella chgalg.
chgalg_persid	chgalg.persid: identificatore unico per questo record nella tabella chgalg, preceduto dall'identificatore di oggetto (chgalg per chgalg) e due punti.
change_id	chgalg.change_id: puntatore per la modifica dell'ID dell'ordine al quale appartiene l'attività. chgalg.change_id = chgalg.id
chgalg_last_mod_dt	chgalg.last_mod_dt: l'ultima data/ora modificata (pdmtime).
time_spent	chgalg.time_spent: periodo trascorso per questa attività, memorizzato come numero totale di secondi. Ad esempio, 80 = 1 minuto e 20 secondi.
time_stamp	chgalg.time_stamp: data/ora di attività modificabile dall'utente (pdmtime).
system_time	chgalg.system_time: data/ora di creazione di record (pdmtime).
analista	chgalg.analyst: puntatore UUID all'UUID del contatto che indica l'analista che ha eseguito l'attività. chgalg.analyst = ca_contact.contact_uuid
chgalg_description	chgalg.description: descrizione di testo di questa attività, la quale può essere modificata dall'utente.
action_desc	chgalg.action_desc: descrizione dell'azione automatizzata. Non può essere modificata dall'utente.
tipo	chgalg.type: puntatore di testo a un record nella tabella di tipo attività. chgalg.type = act_type.code
interna	chgalg.internal: flag intero (1 o 0), che indica se questa voce di registro è visibile a tutti o è diretta al solo uso interno.
knowledge_session	chgalg.knowledge_session: ID di una sessione di un utente specifico.
knowledge_tool	chgalg.knowledge_tool: indicatore dello strumento di conoscenza utilizzato per la ricerca, ad esempio NLS_FAQ o EXPERT.

Campo	Commenti
chgalg_analyst_id	chgalg.analyst: puntatore UUID all'UUID del contatto che indica l'analista che ha eseguito l'attività. chgalg.analyst = ca_contact.contact_uuid

View_Change_to_Change_WF

Questa visualizzazione è il risultato dell'unione della visualizzazione View_Change e della tabella wf e fornisce una visualizzazione di base degli Ordini di cambiamento e delle attività del flusso di lavoro. È possibile che questa visualizzazione non includa tutti gli Ordini di cambiamento, in particolare gli Ordini a cui non sono associate attività del flusso di lavoro.

Campo	Commenti
View_Change.*	Visualizza tutti i campi della visualizzazione View_Change definiti in precedenza in questo documento.
wf_id	wf.id: ID univoco del record della tabella wf.
wf_persid	wf.persid: ID univoco del record della tabella wf, preceduto dall'ID oggetto (wf per la tabella wf) e dai due punti (:).
del	wf.del: indicatore booleano. Specifica se il record deve essere visualizzato dall'utente.
object_type	wf.object_type: nome factory utilizzato per identificare il tipo di record (ad esempio, chg) a cui è associata l'attività del flusso di lavoro.
object_id	wf.object_id: ID univoco utilizzato per identificare il record specifico a cui è associata l'attività del flusso di lavoro. wf.object_id = chg.id
attività	wf.task: ID che indica il tipo di attività rappresentato dal record. wf.task = tskty.code
wf_template	wf.wf_template: ID che indica il tipo di modello con cui è stato creato il record attività del flusso di lavoro. wf.wf_template = wftpl.id
sequenza	wf.sequence: numero intero che indica l'ordine in cui CA SDM deve visualizzare ed eseguire questo particolare record attività del flusso di lavoro (ad esempio, crescente).
wf_status	wf.status: ID che fa riferimento a un record tskstat che indica lo stato corrente dell'attività del flusso di lavoro. wf.status = tskstat.code

Campo	Commenti
group_task	wf.group_task: indicatore booleano che specifica se l'attività appartiene a un gruppo.
asset	wf.asset: identificatore univoco universale (UUID) binario che indica un record della tabella ca_owned_resource. wf.asset = ca_owned_resource.own_resource_uuid
autore	wf.creator: identificatore univoco universale (UUID) binario che indica un record della tabella ca_contact. Specifica la persona che ha creato l'attività del flusso di lavoro. wf.creator = ca_contact.contact_uuid
date_created	wf.date_created: data/ora in cui è stata creata l'attività del flusso di lavoro (pdmtime).
wf_assignee	wf.assignee: identificatore univoco universale (UUID) binario che indica un record della tabella ca_contact. Specifica la persona che è attualmente assegnata all'attività del flusso di lavoro. wf.assignee = ca_contact.contact_uuid
done_by	wf.done_by: identificatore univoco universale (UUID) binario che indica un record della tabella ca_contact. Specifica la persona che ha completato o approvato l'attività del flusso di lavoro. wf.done_by = ca_contact.contact_uuid
wf_start_date	wf_start_date: data e ora in cui l'attività del flusso di lavoro è passata a uno stato più attivo (pdmtime).
wf_est_comp_date	wf.est_comp_date: timestamp (pdmtime) in cui è previsto il completamento dell'attività.
est_duration	wf.est_duration: durata stimata dell'attività del flusso di lavoro.
completion_date	wf.completion_dat: timestamp (pdmtime) in cui è stata completata l'attività del flusso di lavoro.
actual_duration	wf.actual_duration: quantità di tempo effettiva necessaria per il completamento dell'attività del flusso di lavoro.
wf_est_cost	wf.est_cost: costo stimato dell'attività del flusso di lavoro.
costo	wf.cost: costo effettivo richiesto per completare l'attività del flusso di lavoro.
wf_description	wf.description: descrizione dell'attività del flusso di lavoro.
wf_last_mod_dt	wf.last_mod_dt: timestamp (pdmtime) dell'ultima modifica apportata all'attività del flusso di lavoro.

Campo	Commenti
wf_last_mod_by	wf.last_mod_by: ID univoco universale (UUID) binario che fa riferimento a un record della tabella Contatto. Indica l'ultima persona che ha modificato l'attività del flusso di lavoro. wf.last_mod_by = ca_contact.contact_uuid

View_Change_to_Properties

Questa visualizzazione è il risultato dell'unione della visualizzazione View_Change e della tabella prp e fornisce una visualizzazione di base degli Ordini di cambiamento e delle relative proprietà assegnate. È possibile che questa visualizzazione non includa tutti gli Ordini di cambiamento, in particolare gli Ordini a cui non sono associate proprietà.

Campo	Commenti
View_Change.*	Visualizza tutti i campi della visualizzazione View_Change definiti in precedenza in questo documento.
prp_id	prp.id: ID numerico (intero) univoco del record proprietà.
prp_persid	prp.persid: ID univoco del record della tabella wf, preceduto dall'ID oggetto (prp per la tabella prp) e dai due punti (:).
object_type	prp.object_type: nome factory utilizzato per identificare il tipo di record (ad esempio, chg) a cui è associato il record proprietà.
object_id	prp.object_id: ID univoco utilizzato per identificare il record specifico a cui è associata la proprietà. prp.object_id = chg.id
sequenza	prp.sequence: numero intero che indica l'ordine in cui CA SDM deve visualizzare questo particolare record proprietà (ad esempio, crescente).
proprietà	prp.property: ID che indica un record della tabella prptpl. Rappresenta il modello utilizzato per creare la proprietà. prp.property=prptpl.code
valore	prp.value: valore immesso dall'utente in risposta ai campi prp_description e prp.label.
prp_last_mod_dt	prp.last_mod_dt: timestamp (pdmtime) dell'ultima modifica apportata alla proprietà.
prp_last_mod_by	prp.last_mod_by: ID binario che fa riferimento a un record della tabella ca_contact. Indica l'ultima persona che ha modificato il record. prp.last_mod_by = ca_contact.contact_uuid
required	prp.required: indicatore booleano che specifica se la proprietà deve avere un valore prp.value prima del salvataggio del record.

Campo	Commenti
esempio	prp.sample: campo di testo che riporta valori di esempio per aiutare gli utenti a immettere il valore più appropriato in prp.value.
prp_description	prp.description: campo di testo che definisce il tipo di valore che è necessario immettere in prp.value.
etichetta	prp.label: descrizione breve di ciò che è necessario immettere nel campo prp.value.

View_Contact_Full

I campi illustrati di seguito riportano la descrizione della visualizzazione di base di tutti i contatti. La visualizzazione elenca tutti i campi della tabella ca_contact e i campi a cui si fa riferimento, ad esempio le descrizioni brevi di tipo di contatto, nome ubicazione, nomi organizzazioni e tipo servizio per ogni contatto. Questa visualizzazione è stata già unita alle tabelle ca_location, ca_organization, srv_desc e ca_contact_type per fornire i nomi e i simboli effettivi per alcuni dei campi della tabella dei contatti ca_contact. I nomi e i simboli effettivi si trovano alla fine dell'elenco dei campi della visualizzazione.

Campo	Commenti
contact_uuid	ca_contact.contact_uuid: ID univoco binario di ciascun record ca_contact.
middle_name	ca_contact. middle_name: secondo nome del contatto.
alias	ca_contact.alias: nome alternativo, spesso informale, del contatto.
last_name	ca_contact.last_name: cognome del contatto.
first_name	ca_contact.first_name: nome formale del contatto.
pri_phone_number	ca_contact.pri_phone_number: numero di telefono principale del contatto.
alt_phone_number	ca_contact.alt_phone_number: numero di telefono alternativo del contatto.
fax_number	ca_contact.fax_number: numero di fax del contatto.
mobile_phone	ca_contact.mobile_phone: numero di cellulare del contatto.
pager_number	ca_contact.pager_number: numero di cercapersone del contatto.
email_address	ca_contact.email_address: indirizzo di posta elettronica del contatto.
location_uuid	ca_contact.location_uuid: ID univoco binario che fa riferimento a un record della tabella ca_location. Indica l'ubicazione statica del contatto. ca_contact.location_uuid = ca_location.location_uuid

Campo	Commenti
floor_location	ca_contact.floor_location: piano dell'edificio del contatto.
pager_email_address	ca_contact.pager_email_address: indirizzo di posta elettronica del contatto correlato al cercapersone.
room_location	ca_contact.room_location: stanza del contatto presso il piano dell'edificio in cui si trova l'ubicazione statica.
contact_type	ca_contact.contact_type: ID numerico (intero) univoco che fa riferimento a una riga della tabella ca_contact_type. Indica la funzione generale del contatto nell'ambito dell'applicazione Service Desk. ca_contact.contact_type = ca_contact_type.id
non attivo	ca_contact.inactive: indicatore booleano che indica lo stato del record. Determina l'inclusione o l'esclusione del record dalle ricerche standard nell'ambito del service desk.
creation_user	ca_contact.creation_user: ID utente del contatto che ha creato il record. ca_contact.creation_user = ca_contact.userid
creation_date	ca_contact.creation_date: timestamp (pdmtime) che indica la data e l'ora di creazione del contatto.
last_update_user	ca_contact.last_update_user: ID utente del contatto che ha effettuato l'ultimo aggiornamento del record del contatto. ca_contact.last_update_user = ca_contact.userid
last_update_date	ca_contact.last_update_date: timestamp (pdmtime) che indica la data e l'ora dell'ultima modifica del record.
version_number	ca_contact.version number: indicatore della versione interna.
reparto	ca_contact.department: ID numerico (intero) univoco che fa riferimento a una riga della tabella ca_resource_department. Indica il reparto del contatto. ca_contact.department = ca_resource_department.id
commento	ca_contact.comment: campo di testo libero per i commenti degli analisti su fattori importanti che possono influenzare la gestione del particolare contatto.
company_uuid	ca_contact.company_uuid: ID univoco binario che fa riferimento a una riga della tabella ca_company. Indica il rapporto tra il contatto e la società. ca_contact.company_uuid = ca_company.company_uuid
organization_uuid	ca_contact.organization_uuid: ID univoco binario che fa riferimento a una riga della tabella ca_organization. Indica l'organizzazione in cui lavora il contatto. ca_contact.organizaiton_uuid = ca_organization.organization_uuid

Campo	Commenti
admin_organization_uuid	ca_contact.admin_organization_uuid: ID univoco binario che fa riferimento a una riga della tabella ca_organization. Indica l'organizzazione amministrativa del contatto. ca_contact.admin_organization_uuid = ca_organization.organization_uuid
alternate_identifier	ca_contact.alternate_identifier: ID definito dall'utente. Solitamente, un'entità utilizzata dalle risorse umane per identificare in modo univoco il contatto.
job_title	ca_contact.job_title: ID numerico (intero) univoco che fa riferimento alla tabella ca_job_title. Indica la qualifica professionale standard del contatto. ca_contact.job_title = ca_job_title.id
job_function	ca_contact.job_function: ID numerico (intero) univoco che fa riferimento alla tabella ca_job_function. Indica una descrizione generica standard delle mansioni professionali del contatto. ca_contact.job_function = ca_job_function.id
mail_stop	ca_contact.mail_stop: casella postale.
cost_center	ca_contact.cost_center: ID numerico (intero) univoco che fa riferimento alla tabella ca_resource_cost_center. Indica il centro di costo principale del contatto. ca_contact.cost_center = ca_cost_center.id
id utente	ca_contact.userid: ID utente che il contatto utilizza per accedere a Service Desk.
supervisor_contact_uuid	ca_contact.supervisor_contact_uuid: ID univoco binario che fa riferimento a una riga della tabella ca_contact. Crea una gerarchia di contatti per indicare la struttura di report di ciascun contatto. ca_contact.supervisor_contact_uuid = ca_contact.contact_uuid
exclude_registration	ca_contact.exclude registration: flag interno.
delete_time	ca_contact.delete_time: timestamp che indica quando il flag "non attivo" è stato impostato su 1.
contact_type_name	ca_contact_type.name: descrizione breve di ca_contact.contact_type del contatto.
location_name	ca_location.name: descrizione breve della posizione statica del contatto.
organization	ca_organization.org_name: descrizione breve di ca_contact.organizaiton_uuid del contatto.
admin_organization	ca_organization.org_name: descrizione breve del nome dell'organizzazione di questo contatto. ca_contact.admin_organization_uuid:

Campo	Commenti
service_type	srv_desc.sym: descrizione breve di usp_contact.c_service_type del contatto. ca_contact.contact_uuid = usp_contact.contact_uuid E usp_contact.c_service_type = srv_desc.code
state_sym	ca_location.state: ID numerico (intero) univoco che fa riferimento a una riga della tabella ca_state_provice. Indica lo stato, la provincia o un'altra area geografica definita manualmente. ca_contact.location_uuid = ca_location.location_uuid E ca_location.state = ca_state_province.id

View_Contact_to_Environment

Il seguente elenco di campi rappresenta una visualizzazione di base dei contatti e del relativo ambiente (asset). Si tratta di una visualizzazione della tabella (ca_contact), ma è anche il risultato dell'unione con la tabella ca_owned_resource e fornisce un elenco di tutti gli asset associati a un contatto. Questa visualizzazione può essere unita alla visualizzazione View_Contact_Full per ottenere il tipo di contatto, il tipo di servizio, le organizzazioni e l'ubicazione di ciascun contatto. Per ottenere le stesse informazioni è anche possibile unire questa visualizzazione ad altre singole tabelle.

Campo	Commenti
ca_contact.*	I campi ca_contact definiti nella definizione di visualizzazione View_Contact_Full.
asset_uuid	ca_owned_resource.own_resource_uuid: ID univoco binario di un asset della tabella ca_owned_resource.
asset_name	ca_owned_resource.resource_name: nome di rete designato per l'asset.

View_Group

Di seguito è riportata la visualizzazione di base della tabella Contatto. Questa visualizzazione elenca solo i contatti di tipo gruppo. L'ID del tipo contatto è 2308, che indica il tipo "gruppo". È possibile unire questa visualizzazione ad altre tabelle di CA SDM per ottenere dati più significativi per le segnalazioni. Ad esempio, è possibile unire questa visualizzazione alla tabella Posizione (ca_location) per trovare il nome e l'indirizzo effettivi dell'ubicazione del gruppo. È possibile anche unire questa visualizzazione alla tabella Organizzazione (ca_organization) per ottenere i nomi dell'organizzazione funzionale e di amministrazione del gruppo.

Campo	Commenti
ca_contact.*	I campi ca_contact definiti nella definizione di visualizzazione View_Contact_Full.

Di seguito è riportato un esempio che spiega il funzionamento dell'unione delle tabelle e come vengono estratti i campi di report. Il campo di una tabella (a destra) viene unito (->) al campo di un'altra tabella (a sinistra). Per una corretta unione di tabelle e visualizzazioni, è necessario conoscere le differenze con il concetto di "unione" nell'ambito dei database. I campi definiti nelle parentesi, come indicato di seguito, rappresentano gli elementi che si desidera includere nei rapporti se le tabelle precedenti vengono unite alla visualizzazione View_Group:

- View_Group.contact_type -> ca_contact_type.id (ca_contact_type.sym)
- View_Group.location_uuid -> ca_location.location_uuid (ca_location.location_name)
- View_Group.organization_uuid -> ca_organization.organization_uuid (ca_organization.org_name)
- View_Group.admin_organization_uuid -> ca_organization(2).organization_uuid (ca_organization(2). org_name)

View_Group_to_Contact

Di seguito è riportata la visualizzazione di base di tutti i contatti dei gruppi (membri). La visualizzazione include anche i responsabili. La visualizzazione View_Group viene unita alla tabella Group_Member e quindi alla tabella ca_contact. Vengono riportati tutti i campi della visualizzazione View_Group e il nome, il secondo nome e il cognome della tabella ca_contact. Viene anche descritto il flag Group_Member relativo al responsabile. Il flag del responsabile dei membri del gruppo è 1 oppure 0, per indicare che il membro è (1 - sì) un responsabile oppure (0 - no) un altro tipo di membro. La maggior parte delle informazioni di questa visualizzazione è correlata al gruppo nel suo insieme e non ai membri effettivi. La visualizzazione viene utilizzata per trovare informazioni su un particolare gruppo e include i nomi dei membri.

Campo	Commenti
View_Group.*	I campi View_Group indicati nella definizione di View_Group.
member_lastname	ca_contact.last_name: cognome del membro del gruppo.
member_firstname	ca_contact.first_name: nome formale del membro del gruppo.
member_middlename	ca_contact.middle_name: secondo nome del membro del gruppo.
grpmem_manager_flag	ca_contact.manager_flag: indicatore del responsabile dei membri del gruppo (1 oppure 0).

View_Issue

Di seguito si riporta la visualizzazione di base di tutte le Issue. In questa visualizzazione vengono mostrati lo stato, la priorità, la categoria, le organizzazioni, il nome completo del richiedente, il nome completo dell'assegnatario, il nome del gruppo, l'ID e così via. La tabella Issue è stata unita con altre tabelle per fornire altri dati più significativi relativi alle Issue.

Campo	Commenti
id	issue.id: ID univoco del record della tabella Issue.
persid	issue.persid: ID univoco del record della tabella Issue, preceduto dall'ID dell'oggetto (iss per la tabella Issue) e dal segno due punti (:).
issue_ref_num	issue.iss_ref_num: numero di riferimento della Issue utilizzato dagli analisti e dai clienti per fare riferimento a una particolare Issue.
description	issue.description: descrizione estesa di una Issue, come specificata da un analista o cliente.
status	issue.status: ID univoco dello stato di uno stato Issue che rinvia alla tabella issstat. issue.status = issstat.code
active_flag	issue.active_flag: flag numerico utilizzato per determinare se la Issue è attiva (1 o 0).
start_date	issue.start_date: data in cui la prima attività è passata allo stato In sospeso (pdmtime).
open_date	issue.open_date: data di creazione della Issue (pdmtime).
last_mod_dt	issue.last_mod_dt: data dell'ultima modifica (pdmtime).
last_mod_by	issue.last_mod_by: punta all'UUID del contatto che indica l'ultimo contatto che ha modificato la Issue. issue.last_mod_by = ca_contact.contact_uuid
close_date	issue.close_date: data in cui la Issue è stata impostata su Non attiva (pdmtime).
resolve_date	issue.resolve_date: data in cui la Issue è stata impostata su uno stato configurato per indicare che la Issue è stata risolta (pdmtime).
rootcause	issue.rootcause: puntatore a un record nella tabella rootcause che rappresenta il motivo della registrazione della Issue. issue.rootcause = rootcause.id
est_total_time	issue.est_total_time: tempo totale stimato (pdmtime) per il completamento della Issue.

Campo	Commenti
actual_total_time	issue.actual_total_time actual: tempo totale effettivo (pdmtime) per il completamento della Issue.
log_agent	issue.log_agent: ID binario univoco relativo alla tabella ca_contact che, a sua volta, fa riferimento alla persona che ha creato la Issue. issue.log_agent = ca_contact.contact_uuid
assignee	issue.assignee: puntatore all'UUID del contatto assegnato all'Ordine di cambiamento. issue.assignee = ca_contact.contact_uuid
organization	issue.organization: puntatore all'UUID dell'organizzazione interna che rappresenta l'organizzazione di appartenenza della Issue. issue.organization = ca_organization.organization_uuid
group_id	issue.group_id: puntatore all'UUID del contatto che rappresenta il gruppo assegnato alla Issue. issue.group_id = ca_contact.contact_uuid
affected_contact	issue.affected_contact: puntatore all'UUID del contatto che rappresenta il contatto interessato dalla Issue. issue.affected_contact = ca_contact.contact_uuid
requestor	issue.requrestor: puntatore all'UUID del contatto che rappresenta la persona che ha richiesto la registrazione della Issue. issue.requestor = ca_contact.contact_uuid
category	issue.category: puntatore al codice categoria della Issue che indica la categoria di appartenenza della Issue. issue.category = isscat.code
priority	issue.priority: puntatore all'enumerazione di priorità, che rappresenta la priorità associata alla Issue. issue.priority = pri.enum
need_by	issue.need_by: data che indica quando l'utente finale interessato (affected_end_user) desidera che venga completata la Issue (pdmtime).
est_comp_date	issue.est_comp_date: data stimata di completamento (pdmtime) della Issue.
actual_comp_date	issue.actual_comp_date: data effettiva di completamento (pdmtime) della Issue.
est_cost	issue.est_cost: costo stimato della Issue.
actual_cost	issue.actual_cost: costo effettivo dell'implementazione della Issue.
justification	issue.justification: campo di testo che consente al richiedente di specificare il motivo della Issue.
backout_plan	issue.backout_plan: campo di testo che consente a un analista di specificare un piano alternativo per la Issue.

Campo	Commenti
impact	issue.impact: puntatore a un record della tabella Impatto che indica l'ambito delle risorse interessate dalla modifica. issue.impact = impact.enum
parent	issue.parent: puntatore a un ID Issue diverso che consente di creare una gerarchia di Issue. issue.parent = issue.id
effort	issue.effort: campo di testo contenente la descrizione del piano di implementazione della Issue.
support_lev	issue.support_lev: puntatore a un record di Service Desk che automatizza alcuni vincoli richiesti per il completamento della Issue. issue.support_lev = srv_desc.code
template_name	issue.template_name: puntatore a un modello di Issue e al relativo nome. issue.template_name = iss_template.template_name
sla_violation	issue.sla_violation: numero intero che indica il numero di violazioni SLA associate alla Issue.
predicted_sla_viol	issue.predicted_sla_viol: campo con tecnologia Neugent (r5.5)
macro_predict_viol	issue.macro_predict_viol: campo con tecnologia Neugent (r5.5)
created_via	issue.created_via: puntatore a un record della tabella interface. Indica l'interfaccia di provenienza della Issue. issue.created_via = interface.id
call_back_date	issue.call_back_date: campo di data/ora (pdmtime) che indica la data/ora futura in cui dovrà essere contattato il richiedente.
call_back_flag	issue.call_back_flag: indicatore booleano visualizzato in formato di casella di controllo che indica se inviare una notifica all'analista nella data specificata in issue.call_back_date.
string1	Campo di testo definibile dall'utente.
string2	Campo di testo definibile dall'utente.
string3	Campo di testo definibile dall'utente.
string4	Campo di testo definibile dall'utente.
string5	Campo di testo definibile dall'utente.
string6	Campo di testo definibile dall'utente.
service_date	issue.service_date: data e ora (pdmtime) in cui si prevede che il vendor si occupi della Issue.
service_num	issue.service_num: campo di testo in cui indicare il numero di ordine di acquisto o di assistenza del vendor esterno.

Campo	Commenti
product	issue.product: puntatore a un record nella tabella Prodotto che indica il prodotto interessato dalla modifica. issue.product = product.id
actions	issue.actions: campo di testo esteso per la documentazione delle azioni.
type_of_contact	issue.type_of_contact: puntatore a un record nella tabella toc che indica la classificazione generale dal punto di vista dell'utente finale interessato (affected_end_user) in merito alla Issue. issue.type_of_contact = toc.id
reporting_method	issue.reporting_method: puntatore a un record della tabella repmeth selezionato dalla persona che crea la Issue per classificarne l'origine. issue.reporting_method = repmeth.id
person_contacting	issue.person_contacting: puntatore a un record della tabella perscon che indica il ruolo dell'utente finale (affected_end_user) interessato o del richiedente. issue.person_contacting = perscon.id
status_name	issstat.sym: descrizione dello stato visualizzata dall'utente. issue.status = issstat.code
priority_num	pri.sym: descrizione della priorità visualizzata dall'utente. issue.priority = pri.enum
category_name	isscat.sym: nome della categoria di modifica visualizzato dall'utente. issue.category = isscat.code
organization_name	ca_organization.org_name: nome di un'organizzazione visualizzato dall'utente. issue.organization = ca_organization.organization_uuid
affected_end_user_lastname	ca_contact.last_name: cognome dell'utente finale interessato. issue.affected_end_user = ca_contact.contact_uuid
affected_end_user_firstname	ca_contact.first_name: nome dell'utente finale interessato. issue.affected_end_user = ca_contact.contact_uuid
affected_end_user_middlename	ca_contact.middle_name: secondo nome dell'utente finale interessato. issue.affected_end_user = ca_contact.contact_uuid
assignee_lastname	ca_contact.last_name: cognome dell'assegnatario. issue.assignee = ca_contact.contact_uuid
assignee_firstname	ca_contact.first_name: nome dell'assegnatario. issue.assignee = ca_contact.contact_uuid
assignee_middlename	ca_contact.middle_name: secondo nome dell'assegnatario. issue.assignee = ca_contact.contact_uuid
groupID	View_Group.contact_uuid: rappresentazione binaria dell'ID interno utilizzato per il gruppo assegnato alla Issue. issue.group_id = ca_contact.contact_uuid

Campo	Commenti
group_name	View_Group.last_name: nome del gruppo assegnato alla Issue. issue.group = ca_contact.contact_uuid
service_type	srv_desc.sym: nome del tipo di servizio applicato a questa Issue. issue.support_lev = srv_desc.code
impact_num	impact.sym: descrizione dell'impatto visualizzata dagli utenti. issue.impact = impact.enum
product_sym	product.sym: descrizione del prodotto visualizzata dagli utenti. issue.product = product.id
type_of_contact_sym	toc.sym: descrizione del tipo di contatto visualizzata dagli utenti. issue.type_of_contact = toc.id
rpting_method_sym	repmeth.sym: descrizione del metodo di reporting dal punto di vista dell'utente. issue.reporting_method = repmeth.id
person_contacting_sym	perscon.sym: descrizione della persona di contatto visualizzata dagli utenti. issue.person_contacting = perscon.id
created_via_sym	interface.sym: issue.created_via = interface.id.
rootcause_sym	rootcause.sym: issue.rootcause = rootcause.id.

View_Issue_Act_Log

Di seguito è riportata la descrizione della visualizzazione di base di tutti i registri delle attività correlate alle Issue. Si tratta di una visualizzazione della tabella issalg unita alle tabelle act_type e ca_contact per fornire dati più significativi, quali il tipo effettivo di attività e il nome completo dell'analista che ha eseguito l'attività.

Campo	Commenti
id	issalg.id: identificatore unico per questo record nella tabella issalg.
persid	issalg.persid: identificatore unico per questo record nella tabella issalg, preceduto dall'identificatore di oggetto (issalg per issalg) e due punti.
issue_id	issalg.issue_id: puntatore all'ID Issue a cui appartiene questa attività. issalg.issue_id = issalg.id
last_mod_dt	issalg.last_mod_dt: l'ultima data/ora modificata (pdmtime).
time_spent	issalg.time_spent: periodo trascorso per questa attività, memorizzato come numero totale di secondi. Ad esempio, 80 = 1 minuto e 20 secondi.
time_stamp	issalg.time_stamp: data/ora di attività modificabile dall'utente (pdmtime).

Campo	Commenti
system_time	issalg.system_time: data/ora di creazione di record (pdmtime).
analista	issalg.analyst: ID binario univoco relativo all'UUID contatto che indica l'analista che ha eseguito l'attività. issalg.analyst = ca_contact.contact_uuid
description	issalg.description: descrizione di testo di questa attività, la quale può essere modificata dall'utente.
action_desc	issalg.action_desc: descrizione di testo dell'azione automatica, la quale non può essere modificata dall'utente.
tipo	issalg.type: puntatore di testo a un record nella tabella di tipo attività. issalg.type = act_type.code
interna	issalg.internal: flag intero (1 o 0), che indica se questa voce di registro è visibile a tutti o è diretta al solo uso interno.
knowledge_session	issalg.knowledge_session: identificatore per una sessione particolare di un utente particolare.
knowledge_tool	issalg.knowledge_tool: indicatore dello strumento della conoscenza utilizzato per la ricerca, ad esempio NLS_FAQ, EXPERT e così via.
analyst_lastname	View_Contact_Full.last_name: cognome dell'analista derivante da issalg.analyst = ca_contact.contact_uuid.
analyst_firstname	View_Contact_Full.first_name: il nome dell'analista.
analyst_middlename	View_Contact_Full.middle_name: secondo nome dell'analista.
activity_type	act_type.sym: tipo di attività a cui si fa riferimento tramite issalg.type = act_type.code.

View_Issue_to_Assets

Il seguente elenco di campi rappresenta una visualizzazione di base delle Issue e dei relativi asset. La tabella issue è indirettamente unita alla tabella ca_owned_resource, e ad altre tabelle correlate agli asset, per ottenere un elenco degli asset di ciascuna Issue. È possibile che non vengano elencate tutte le Issue, in particolare quelle a cui non sono associati asset.

Campo	Commenti
View_Issue.*	La visualizzazione View_Issue che definisce tutti i campi elencati nella visualizzazione View_Issue.
assetID	ca_owned_resource.own_resource_uuid - Campo binario che funziona come identificativo univoco interno, non modificabile, del record di un asset.

Campo	Commenti
asset_serial_num	ca_owned_resource.serial_number - Numero di serie del record di un asset.
asset_class	ca_resource_class.name - Breve descrizione della classe di appartenenza dell'asset. ca_owned_resource.resource_class = ca_resource_class.id
asset_family	ca_resource_family.name - Famiglia di asset a cui appartiene l'asset. ca_owned_resource.resource_class = ca_resource_class.id e ca_resource_class.family_id = ca_resource_family.id
asset_name	ca_owned_resource.resource_name - Nome di rete con il quale è noto l'asset.

View_Issue_to_Issue_Act_Log

Di seguito è riportata la descrizione della visualizzazione di base di tutte le Issue e dei relativi registri delle attività. Questa visualizzazione è il risultato dell'unione delle visualizzazioni View_Issue e View_Issue_Act_Log e fornisce informazioni dettagliate sulle Issue e sui relativi registri delle attività. I dati effettivi si trovano in fondo all'elenco dei campi.

Campo	Commenti
View_Issue.*	Fare riferimento alla visualizzazione View_Issue, descritta in precedenza in questo documento.
issalg_id	issalg.id: identificatore unico per questo record nella tabella issalg.
issalg_persid	issalg.persid: identificatore unico per questo record nella tabella issalg, preceduto dall'identificatore di oggetto (issalg per issalg) e due punti.
issue_id	issalg.issue_id: puntatore all'ID Issue a cui appartiene questa attività. issalg.issue_id = issalg.id
issalg_last_mod_dt	issalg.last_mod_dt: l'ultima data/ora modificata (pdmtime).
time_spent	issalg.time_spent: periodo trascorso per questa attività, memorizzato come numero totale di secondi. Ad esempio, 80 = 1 minuto e 20 secondi.
time_stamp	issalg.time_stamp: data/ora di attività modificabile dall'utente (pdmtime).
system_time	issalg.system_time: data/ora di creazione di record (pdmtime).

Campo	Commenti
analista	issalg.analyst: puntatore binario unico all'uuid di contatto per ottenere l'analista che ha eseguito l'attività. issalg.analyst = ca_contact.contact_uuid
issalg_description	issalg.description: descrizione di testo di questa attività, la quale può essere modificata dall'utente.
action_desc	issalg.action_desc: descrizione di testo dell'azione automatica, la quale non può essere modificata dall'utente.
tipo	issalg.type: puntatore di testo a un record nella tabella di tipo attività. issalg.type = act_type.code
interna	issalg.internal: flag intero (1 o 0), che indica se questa voce di registro è visibile a tutti o è diretta al solo uso interno.
knowledge_session	issalg.knowledge_session: identificatore per una sessione particolare di un utente particolare.
knowledge_tool	issalg.knowledge_tool: indicatore dello strumento della conoscenza utilizzato per la ricerca, ad esempio NLS_FAQ, EXPERT e così via.
issalg_analyst_id	issalg.analyst: puntatore binario unico all'uuid di contatto per ottenere l'analista che ha eseguito l'attività. issalg.analyst = ca_contact.contact_uuid

View_Change_to_Request

Di seguito è riportata la descrizione della visualizzazione di base degli Ordini di cambiamento a cui sono assegnate solo richieste. Questa visualizzazione è il risultato dell'unione della visualizzazione View_Change con la tabella Richiesta (call_req) e fornisce i dettagli sull'Ordine di cambiamento e sulla Richiesta associata.

Campo	Commenti
View_Change.*	Visualizza tutti i campi della visualizzazione View_Change definiti in precedenza in questo documento.
cr_id	call_req.id: identificatore unico per questo record nella tabella call_req.
ref_num	call_req.ref_num: numero di riferimento della richiesta utilizzato da analisti e clienti per fare riferimento a una richiesta specifica.
cr_summary	call_req.summary: breve descrizione della richiesta per riferimento rapido.

Campo	Commenti
cr_persid	call_req.persid: identificatore unico per questo record nella tabella call_req, preceduto dall'identificatore di oggetto (cr per la tabella call_req) e due punti.
cr_description	call_req.description: descrizione lunga di una richiesta, stabilita da un analista o cliente.
cr_status	call_req.status: identificatore unico riferito a un record nella tabella cr_stat. che indica lo stato della richiesta: call_req.status = cr_stat.code
cr_active_flag	call_req.active_flag: flag numerico utilizzato per determinare se il record della richiesta è attivo (1 o 0).
time_spent_sum	call_req.time_spent_sum: totale risultante da tutti i campi time_spent dei record della tabella act_log espresso in secondi (ad esempio, 80 = 1 minuto e 20 secondi).
cr_open_date	call_req.open_date: data e ora di creazione della richiesta (pdmtime).
cr_last_mod_dt	call_req.last_mod_dt: ultima data e ora modificata (pdmtime).
cr_close_date	call_req.close_date: data e ora in cui la richiesta è stata impostata come non attiva (pdmtime).
cr_log_agent	call_req.log_agent: ID binario univoco relativo alla tabella ca_contact. Indica la persona che ha creato in origine la richiesta. call_req.log_agent = ca_contact.contact_uuid
cr_group_id	call_req.group_id: ID binario univoco relativo a un record della tabella ca_contact. Indica il gruppo attualmente assegnato alla richiesta. call_req.group_id = ca_contact.contact_uuid
cr_assignee	call_req.assignee: ID binario univoco relativo a un record della tabella ca_contact. Indica la persona attualmente assegnata alla richiesta. call_req.assignee = ca_contact.contact_uuid
cliente	call_req.customer: ID binario univoco relativo a un record della tabella ca_contact. Indica l'utente finale interessato dalla richiesta. call_req.customer = ca_contact.contact_uuid
charge_back_id	charge_back_id: campo di testo disponibile per l'uso come indicatore di linguaggio di contabilità per l'assegnazione della spesa di questa richiesta al centro di costo appropriato.
affected_rc	call_req.affected_rc: ID binario univoco relativo a una riga della tabella ca_owned_resource. Indica l'asset a cui si riferisce la richiesta. call_req.affected_rc = ca_owned_resource.own_resource_uuid.
cr_support_lev	call_req.support_lev: puntatore a un record di descrizione di servizio, il quale automatizza alcuni vincoli per i quali è necessario completare questa richiesta. call_req.support_lev = srv_desc.code

Campo	Commenti
cr_category	call_req.category: identificatore unico riferito a un record nella tabella prob_cgt. Indica la categoria a cui appartiene la richiesta. call_req.category = prob_ctg.persid
soluzione	call_req.solution: puntatore per la richiesta di soluzione. call_req.solution = crsol.persid
cr_impact	call_req.impact: ID numerico univoco relativo a una riga della tabella impact. che indica la portata della richiesta. call_req.impact = impact.enum
cr_priority	call_req.priority: ID numerico univoco relativo a un record della tabella pri. Indica il modo in cui gli analisti assegnano la priorità alle attività associate alla richiesta. call_req.priority = pri.enum
urgenza	call_req.urgency: ID numerico univoco relativo a una riga della tabella urgency. che indica l'urgenza espressa dall'utente per la soluzione della richiesta. call_req.urgency = urgncy.enum
gravità	call_req.severity: ID numerico univoco relativo a una riga della tabella severity. Indica il livello di gravità delle conseguenze della mancata risoluzione della richiesta. call_req.severity = sevrty.enum
extern_ref	Specifica un ticket associato.
last_act_id	ID associato all'ultima attività eseguita.
cr_tticket	Puntatore a un trouble ticket che consente di visualizzare il ticket associato.
cr_parent	call_req.parent: puntatore persid a un altro persid di Richiesta che facilita la creazione di una gerarchia di Ordini di cambiamento. call_req.parent = call_req.persid
cr_template_name	call_req.template_name: valore di testo indicante che questa richiesta è designata e può essere scelta da un elenco come modello per altre richieste simili. cr_template.template = call_req.persid
cr_sla_violation	call_req.sla_violation: numero intero che indica il numero di violazioni SLA associate alla richiesta.
cr_predicted_sla_viol	call_req.predicted_sla_viol: campo con tecnologia Neugent (r5.5).
cr_created_via	call_req.created_via: puntatore numerico a un record della tabella di interfaccia. che indica l'interfaccia dalla quale è stato creato l'Ordine di cambiamento. call_req.created_via = interface.id
cr_call_back_date	call_req.call_back_date: campo di timestamp che indica la data e l'ora (pdmtime) entro la quale contattare l'utente finale interessato (affected_end_user).

Campo	Commenti
cr_call_back_flag	call_req.call_back_flag: indicatore booleano visualizzato come casella di controllo che indica se inviare una notifica all'analista nella data specificata in call_req.call_back_date.
event_token	call_req.event_token: usato da CA NSM per l'abbinamento dei messaggi.
tipo	call_req.type: campo di testo riferito a un record nella tabella crt. che indica il tipo ITIL della richiesta. call_req.type = crt.code
cr_string1	Stringa definibile dall'utente.
cr_string2	Stringa definibile dall'utente.
cr_string3	Stringa definibile dall'utente.
cr_string4	Stringa definibile dall'utente.
cr_string5	Stringa definibile dall'utente.
cr_string6	Stringa definibile dall'utente.
modifica	call_req.change: ID numerico univoco relativo a una riga della tabella chg. Indica l'Ordine di cambiamento creato come risultato della Richiesta. call_req.change = chg.id.

View_Issue_to_Issue_WF

Questa visualizzazione è il risultato dell'unione della visualizzazione View_Issue e della tabella isswf e fornisce una visualizzazione di base delle Issue e delle attività del flusso di lavoro. È possibile che questa visualizzazione non elenchi tutte le Issue, in particolare quelle a cui non sono associate attività del flusso di lavoro.

Campo	Commenti
View_Issue.*	Per la descrizione di ciascun campo, fare riferimento alla definizione della visualizzazione View_Issue fornita in precedenza in questo documento.
wf_id	isswf.id: ID univoco di un record della tabella isswf.
wf_persid	isswf.persid: ID univoco del record della tabella isswf, preceduto dall'ID oggetto (isswf) e dai due punti (:).
del	isswf.del: indicatore booleano che stabilisce se il record deve essere visualizzato dall'utente.
object_type	isswf.object_type: nome factory utilizzato per identificare il tipo di record (ad esempio, chg) a cui è associata l'attività del flusso di lavoro.

Campo	Commenti
object_id	isswf.object_id: ID univoco utilizzato per identificare il record specifico a cui è associata l'attività del flusso di lavoro. isswf.object_id = issue.id
attività	isswf.task: ID che indica il tipo di attività rappresentato dal record. isswf.task = tskty.code
wf_template	isswf.wf_template: ID che indica il tipo di modello con cui è stato creato il record attività del flusso di lavoro. isswf.wf_template = wftpl.id
sequenza	isswf.sequence: numero intero che indica l'ordine in cui CA SDM deve visualizzare ed eseguire questo particolare record attività del flusso di lavoro (ad esempio, crescente).
wf_status	isswf.status: ID che indica un record della tabella tskstat. Specifica lo stato corrente dell'attività del flusso di lavoro. isswf.status = tskstat.code
group_task	isswf.group_task: indicatore booleano che specifica se l'attività appartiene a un gruppo.
asset	isswf.asset: identificatore univoco binario che indica un record della tabella ca_owned_resource. isswf.asset = ca_owned_resource.own_resource_uuid
autore	isswf.creator: identificatore univoco binario che indica un record della tabella ca_contact. Specifica la persona che ha creato l'attività del flusso di lavoro. isswf.creator = ca_contact.contact_uuid
date_created	isswf.date_created: data/ora in cui è stata creata l'attività del flusso di lavoro (pdmtime).
wf_assignee	isswf.assignee: identificatore univoco binario che indica un record della tabella ca_contact. Specifica la persona che è attualmente assegnata all'attività del flusso di lavoro. isswf.assignee = ca_contact.contact_uuid
done_by	isswf.done_by: identificatore univoco binario che indica un record della tabella ca_contact. Specifica la persona che ha completato o approvato l'attività del flusso di lavoro. isswf.done_by = ca_contact.contact_uuid
wf_start_date	wf_start_date: data e ora in cui l'attività del flusso di lavoro è passata a uno stato più attivo (pdmtime).
wf_est_comp_date	isswf.est_comp_date: timestamp (pdmtime) che indica per quando è previsto il completamento dell'attività.

Campo	Commenti
est_duration	isswf.est_duration: durata stimata dell'attività del flusso di lavoro.
completion_date	isswf.completion_date: timestamp (pdmtime) che indica quando è stata completata l'attività del flusso di lavoro.
actual_duration	isswf.actual_duration: quantità di tempo effettiva necessaria per il completamento dell'attività del flusso di lavoro.
wf_est_cost	isswf.est_cost: costo stimato dell'attività del flusso di lavoro.
costo	isswf.cost: costo effettivo richiesto per completare l'attività del flusso di lavoro.
wf_description	isswf.description: descrizione dell'attività del flusso di lavoro.
wf_last_mod_dt	isswf.last_mod_dt: timestamp (pdmtime) dell'ultima modifica apportata all'attività del flusso di lavoro.
wf_last_mod_by	isswf.last_mod_by: ID binario univoco che indica un record della tabella Contatto. Specifica l'autore dell'ultima modifica apportata all'attività del flusso di lavoro. isswf.last_mod_by = ca_contact.contact_uuid

View_Issue_to_Properties

Questa visualizzazione è il risultato dell'unione della visualizzazione View_Issue e della tabella issprp e fornisce una visualizzazione di base delle Issue e delle proprietà assegnate. È possibile che questa visualizzazione non elenchi tutte le Issue, in particolare quelle a cui non sono associate proprietà.

Campo	Commenti
View_Issue.*	Per la descrizione di ciascun campo, fare riferimento alla definizione della visualizzazione View_Issue fornita in precedenza in questo documento.
prp_id	issprp.id: ID numerico (intero) univoco del record proprietà.
prp_persid	issprp.persid: ID univoco del record della tabella prp, preceduto dall'ID oggetto (prp) e dai due punti (:).
sequenza	issprp.sequence: numero intero che indica l'ordine in cui CA SDM deve visualizzare questo particolare record proprietà (ad esempio, crescente).
etichetta	issprp.label: descrizione breve di ciò che è necessario immettere nel campo issprp.value.
valore	issprp.value: valore immesso dall'utente in risposta ai campi prp_description e issprp.label.
prp_last_mod_dt	issprp.last_mod_dt: timestamp (pdmtime) dell'ultima modifica apportata alla proprietà.
prp_last_mod_by	issprp.last_mod_by: ID binario che fa riferimento a un record della tabella ca_contact. Indica l'ultima persona che ha modificato il record. issprp.last_mod_by = ca_contact.contact_uuid
required	issprp.required: indicatore booleano che specifica se la proprietà deve avere un valore issprp.value prima del salvataggio del record.
esempio	issprp.sample: campo di testo che riporta valori di esempio per aiutare gli utenti a immettere il valore più appropriato in issprp.value.
owning_iss	issprp.owning_iss: ID univoco utilizzato per identificare il record specifico a cui è associata la proprietà. issprp.object_id = issue.persid
prp_description	issprp.description: campo di testo che definisce il tipo di valore che è necessario immettere in issprp.value.

View_Request

Di seguito è riportata la descrizione della visualizzazione di base di tutte le Richieste. La tabella Request è stata unita ad altre tabelle di CA SDM per fornire informazioni più specifiche, ad esempio il tipo, la gravità, l'urgenza, la categoria e la priorità del servizio richiesto. Sono disponibili anche altre informazioni sulla richiesta elencata. Tutti i campi della tabella Request (call_req) sono selezionati. I campi estratti, come risultato dell'unione delle tabelle, sono riportati alla fine dell'elenco dei campi.

Campo	Commenti
id	call_req.id: identificatore unico per questo record nella tabella call_req.
persid	call_req.persid: identificatore unico per questo record nella tabella call_req, preceduto dall'identificatore di oggetto (cr per la tabella call_req) e due punti.
ref_num	call_req.ref_num: numero di riferimento della richiesta utilizzato da analisti e clienti per fare riferimento a una richiesta specifica.
riepilogo	call_req.summary: breve descrizione della richiesta per riferimento rapido.
description	call_req.description: descrizione lunga di una richiesta, stabilita da un analista o cliente.
status	call_req.status: identificatore unico riferito a un record nella tabella cr_stat. Indica lo stato della richiesta. call_req.status = cr_stat.code
active_flag	call_req.active_flag: flag numerico intero utilizzato per determinare se il record della richiesta è attivo (1 o 0).
open_date	call_req.open_date: data e ora di creazione della richiesta (pdmtime).
time_spent_sum	call_req.time_spent_sum: totale risultante da tutti i campi time_spent dei record della tabella act_log espresso in secondi (ad esempio, 80 = 1 minuto e 20 secondi).
last_mod_dt	call_req.last_mod_dt: ultima data e ora modificata (pdmtime).
close_date	call_req.close_date: data e ora in cui la richiesta è stata impostata come non attiva (pdmtime).
resolve_date	Data di risoluzione della richiesta (pdmtime).
rootcause	Puntatore a rootcause.id.
log_agent	call_req.log_agent: ID binario univoco relativo alla tabella ca_contact. Indica la persona che ha creato in origine la richiesta. call_req.log_agent = ca_contact.contact_uuid

Campo	Commenti
assignee	call_req.assignee: ID binario univoco relativo a un record della tabella ca_contact. Indica la persona attualmente assegnata alla richiesta. call_req.assignee = ca_contact.contact_uuid
group_id	call_req.group_id: ID binario univoco relativo a un record della tabella ca_contact. Indica il gruppo attualmente assegnato alla richiesta. call_req.group_id = ca_contact.contact_uuid
cliente	call_req.customer: ID binario univoco relativo a un record della tabella ca_contact. Indica l'utente finale interessato dalla richiesta. call_req.customer = ca_contact.contact_uuid
charge_back_id	charge_back_id: campo di testo disponibile per l'uso come indicatore di linguaggio di contabilità per l'assegnazione della spesa di questa richiesta al centro di costo appropriato.
affected_rc	call_req.affected_rc: ID binario univoco relativo a una riga della tabella ca_owned_resource. Indica l'asset a cui si riferisce la richiesta. call_req.affected_rc = ca_owned_resource.own_resource_uuid.
support_lev	call_req.support_lev: puntatore a un record di descrizione di servizio, il quale automatizza alcuni vincoli per i quali è necessario completare questa richiesta. call_req.support_lev = srv_desc.code.
category	call_req.category: identificatore univoco riferito a un record nella tabella prob_ctg. Indica la categoria a cui appartiene la richiesta. call_req.category = prob_ctg.persid
soluzione	call_req.solution: puntatore per la richiesta di soluzione. call_req.solution = crsol.persid
impact	call_req.impact: ID numerico (intero) univoco relativo a una riga della tabella Impatto. Indica la portata dell'impatto della richiesta. call_req.impact = impact.enum
priority	call_req.priority: ID numerico (intero) univoco relativo a un record della tabella pri. Indica il modo in cui gli analisti assegnano la priorità alle attività associate alla richiesta. call_req.priority = pri.enum
urgenza	call_req.urgency: ID numerico (intero) univoco relativo a una riga della tabella Urgenza. Indica il livello di urgenza dell'utente che attende la risoluzione della richiesta. call_req.urgency = urgncy.enum
gravità	call_req.severity: ID numerico (intero) univoco relativo a una riga della tabella severity. Indica il livello di gravità delle conseguenze della mancata risoluzione della richiesta. call_req.severity = sevrty.enum

Campo	Commenti
extern_ref	Riferimento esterno a un ticket associato.
last_act_id	Identifica l'ID dell'ultima attività.
cr_tticket	Puntatore al Trouble Ticket per ottenere il ticket associato.
parent	call_req.parent: puntatore persid a un altro persid di Richiesta che facilita la creazione di una gerarchia di Ordini di cambiamento. call_req.parent = call_req.persid
template_name	call_req.template_name: valore di testo indicante che questa richiesta è designata e può essere scelta da un elenco come modello per altre richieste simili. cr_template.template = call_req.persid
sla_violation	call_req.sla_violation: numero intero che indica quante volte sono stati violati gli SLA associati alla richiesta.
predicted_sla_viol	Indica che una Richiesta è stata classificata dai Neugent come possibile violazione SLA.
macro_predicted_violation	Indica che la Richiesta è stata classificata dai Neugent come possibile violazione SLA.
created_via	call_req.created_via: puntatore numerico (intero) a un record della tabella interface. Indica l'interfaccia con cui è stato creato l'Ordine di cambiamento. call_req.created_via = interface.id
call_back_date	call_req.call_back_date: campo di timestamp che indica la data e l'ora (pdmtime) entro la quale contattare l'utente finale interessato (affected_end_user).
call_back_flag	call_req.call_back_flag: indicatore booleano visualizzato come casella di controllo che indica se inviare una notifica all'analista nella data specificata in call_req.call_back_date.
event_token	call_req.event_token: usato da CA NSM per l'abbinamento dei messaggi.
sched_token	call_req.sched_token: usato da CA NSM per l'abbinamento dei messaggi.

Campo	Commenti
tipo	call_req.type: campo di testo riferito a un record nella tabella crt. Indica il tipo ITIL per la richiesta. call_req.type = crt.code
string1	Stringa definibile dall'utente.
string2	Stringa definibile dall'utente.
string3	Stringa definibile dall'utente.
string4	Stringa definibile dall'utente.
string5	Stringa definibile dall'utente.
string6	Stringa definibile dall'utente.
Problema	Problema ITIL.
incident_priority	Priorità Incidente ITIL.
Cambiamento	call_req.change: ID numerico univoco relativo a una riga della tabella chg. Indica l'Ordine di cambiamento creato come risultato della Richiesta. call_req.change = chg.id.
service_type	srv_desc.sym: indica il tipo di servizio effettivo. call_req.support_lev = srv_desc.code
severity_num	sevrty.sym: numero di gravità effettivo. call_req.severity = sevrty.enum
urgency_num	urgncy.sym: indica il numero di urgenza effettivo. call_req.urgency = urgncy.enum
category_name	prob_ctg.sym: area di Richiesta effettiva (categoria Problema). call_req.category = prob_ctg.id

Campo	Commenti
asset	ca_owned_resource.resource_name: nome asset effettivo. call_req.affected_rc = ca_owned_resource.own_resource_uuid
impact_num	impact.sym: numero di impatto effettivo. call_req.impact = impact.enum
assignee_lastname	ca_contact.last_name: cognome assegnatario effettivo. call_req.assignee = ca_contact.contact_uuid
assignee_firstname	ca_contact.first_name: nome assegnatario effettivo. call_req.assignee = ca_contact.contact_uuid
assignee_middlename	ca_contact.middle_name: secondo nome assegnatario effettivo. call_req.assignee = ca_contact.contact_uuid
customer_lastname	ca_contact.last_name: cognome effettivo dell'utente finale interessato. call_req.customer = ca_contact.contact_uuid
customer_firstname	ca_contact.first_name: nome effettivo dell'utente finale interessato. call_req.customer.ca_contact.contact_uuid
customer_middlename	ca_contact.middle_name: secondo nome effettivo dell'utente finale interessato. call_req.customer = ca_contact.contact_uuid
group_name	View_Group.last_name: nome gruppo effettivo.
GroupID	View_Group.contact_uuid: ID chiave gruppo effettivo.
status_name	cr_stat.sym: stato effettivo.
priority_num	pri.sym: numero di priorità effettivo.

View_Request_to_Act_Log

Di seguito è riportata la descrizione della visualizzazione di base di tutte le Richieste e dei relativi registri delle attività. Questa visualizzazione è il risultato dell'unione delle visualizzazioni View_Request e View_Act_Log per fornire informazioni più dettagliate su ciascuna attività per Richiesta.

Campo	Commenti
View_Request.*	Fare riferimento alla definizione della visualizzazione View_Request, in precedenza in questo documento, per la descrizione di ciascun campo.
View_Act_Log.*	Fare riferimento alla definizione della visualizzazione View_Act_Log, in precedenza in questo documento, per la descrizione di ciascun campo.

View_Request_to_Properties

Di seguito è riportata la descrizione della visualizzazione di base delle richieste di chiamata e delle relative proprietà. La visualizzazione contiene tutte le informazioni delle tabelle call_req e cr_prp.

Campo	Commenti
View_Request.*	Fare riferimento alla definizione della visualizzazione View_Request, in questo documento, per la descrizione di ciascun campo.
crprp_id	cr_prp.id: ID numerico (intero) univoco del record proprietà.
crprp_persid	cr_prp.persid: ID univoco del record della tabella cr_prp, preceduto dall'ID oggetto (cr_prp) e dai due punti (:).
sequenza	cr_prp.sequence: numero intero che indica l'ordine in cui CA SDM deve visualizzare questo particolare record proprietà (ad esempio, crescente).
etichetta	cr_prp.label: descrizione breve di ciò che è necessario immettere nel campo cr_prp.value.
valore	cr_prp.value: valore immesso dall'utente in risposta ai campi prp_description e cr_prp.label.
crprp_last_mod_dt	cr_prp.last_mod_dt: timestamp (pdmtime) dell'ultima modifica apportata alla proprietà.
crprp_last_mod_by	cr_prp.last_mod_by: ID binario che fa riferimento a un record della tabella ca_contact. Indica l'ultima persona che ha modificato il record. cr_prp.last_mod_by = ca_contact.contact_uuid

Campo	Commenti
required	cr_prp.required: indicatore booleano che specifica se la proprietà deve avere un valore cr_prp.value prima del salvataggio del record.
esempio	cr_prp.sample: campo di testo che riporta valori di esempio per aiutare gli utenti a immettere il valore più appropriato in cr_prp.value.
owning_cr	cr_prp.owning_cr: ID univoco utilizzato per identificare il record specifico a cui è associata la proprietà. cr_prp.object_id = call_req.persid
crprp_description	cr_prp.description: campo di testo che definisce il tipo di valore che è necessario immettere in cr_prp.value.

Appendice C: Gruppi moduli

Questa sezione contiene i seguenti argomenti:

Gruppo Moduli cliente (a pagina 1223)
Gruppo moduli dipendente (a pagina 1224)
Gruppo moduli Analista (a pagina 1226)

Gruppo Moduli cliente

I gruppi Moduli cliente comprendono i seguenti moduli Web:

- about.htmpl
- bin_form_np.htmpl
- chg_lr.htmpl
- cr_lr.htmpl
- detail_iss.htmpl
- detail_issalg.htmpl
- detail_KD.htmpl
- generic.htmpl
- home.htmpl
- iss_lr.htmpl
- issue_status_change.htmpl
- list_iss.htmpl
- list_isscat.htmpl
- list_KD.htmpl
- menu_frames.htmpl
- std_body.htmpl
- std_body_site.htmpl
- std_footer.htmpl
- std_footer_site.htmpl
- std_head.htmpl
- std_header.htmpl
- std_head_site.htmpl

Gruppo moduli dipendente

I seguenti moduli Web sono inclusi nei gruppi di moduli Dipendente:

- about.htmpl
- bin_form_np.htmpl
- htmpl |
- change_status_change.htmpl
- chg_lr.htmpl
- cr_lr.htmpl
- detail_alg.htmpl
- detail_chg.htmpl
- detail_chgalg.htmpl
- detail_cr.htmpl
- detail_in.htmpl
- detail_KD.htmpl
- generic.htmpl
- home.htmpl
- iss_lr.htmpl
- list_chg.htmpl
- list_chgcat.htmpl
- list_cr.htmpl
- list_in.htmpl
- list_KD.htmpl
- list_pcat.htmpl
- list_pcat_cr.htmpl
- list_pcat_in.htmpl
- menu_frames.htmpl
- request_status_change.htmpl
- show_error.htmpl
- std_body.htmpl
- std_body_site.htmpl
- std_footer.htmpl
- std_footer_site.htmpl

- std_head.htmpl
- std_header.htmpl
- std_head_site.htmpl

Gruppo moduli Analista

I seguenti moduli Web sono inclusi nei gruppi di moduli Analista:

A

- about.htmpl
- acctyp_role_tab.htmpl
- acctyp_web_auth_tab.htmpl
- acctyp_wsp_tab.htmpl
- admin_empty.htmpl
- admin_main_role.htmpl
- admin_tab_dflt.htmpl
- admin_tree.htmpl
- attmnt_content_tab.htmpl
- attmnt_fields.htmpl
- attmnt_permissions_tab.htmpl
- attmnt_upload_popup.htmpl
- att_mgs_event.htmpl
- att_stype_event.htmpl
- aty_chg_ntfr_tab.htmpl
- aty_chg_svy_tab.htmpl
- aty_cr_ntfr_tab.htmpl
- aty_cr_svy_tab.htmpl
- aty_iss_ntfr_tab.htmpl
- aty_iss_svy_tab.htmpl
- aty_kdComment_ntfr_tab.htmpl
- aty_kd_ntfr_tab.htmpl
- aty_mgs_ntfr_tab.htmpl

B

- bhvtpl_todo_tab.htmpl
- bhvtpl_trans_info_tab.htmpl
- bin_form_np.htmpl

C

- cancel.htmpl
- cancel_empty.htmpl
- category_content_tab.htmpl
- category_permissions_tab.htmpl
- chgcat_auto_assignment_tab.htmpl
- chgcat_prptpl_tab.htmpl
- chgcat_wftpl_tab.htmpl
- chg_accumulate.htmpl
- chg_causedreq_tab.htmpl
- chg_close_all_child.htmpl
- chg_expedite.htmpl
- chg_lr.htmpl
- chg_relchg_tab.htmpl
- chg_relreq_tab.htmpl
- cia_bmhier_tab.htmpl
- cia_export_bmhier.htmpl
- cia_export_nr.htmpl
- cia_nr_tab.htmpl
- cia_pwd_tab.htmpl
- cia_sync_stat.htmpl
- cnote_tracker.htmpl
- cnt_addr_tab.htmpl
- cnt_auto_assignment_tab.htmpl
- cnt_env_tab.htmpl
- cnt_grp_tab.htmpl
- cnt_mem_tab.htmpl
- cnt_notif_tab.htmpl
- cnt_org_tab.htmpl
- cnt_rem_tab.htmpl
- cnt_role_tab.htmpl
- cr_attach_chg.htmpl
- cr_close_all_child.htmpl
- cr_detach_chg.htmpl

- cr_lr.htmpl
- cr_relreq_tab.htmpl

D

- dcon_constraint_tab.htmpl
- dcon_sql_tab.htmpl
- detail.template
- detail_acctyp.htmpl
- detail_act_type_assoc.htmpl
- detail_ADMIN_TREE.htmpl
- detail_alg.htmpl
- detail_arcpur_rule.htmpl
- detail_asset.htmpl
- detail_atev.htmpl
- detail_atomic_cond.htmpl
- detail_attmnt_edit.htmpl
- detail_attmnt_error.htmpl
- detail_attmnt_folder.htmpl
- detail_attmnt_ro.htmpl
- detail_attr_alias.htmpl
- detail_aty.htmpl
- detail_audlog.htmpl
- detail_bhvtpl.htmpl
- detail_bmcls.htmpl
- detail_bmhier.htmpl
- detail_bmrep.htmpl
- detail_BU_TRANS.htmpl
- detail_ca_cmpny.htmpl
- detail_chg.htmpl
- detail_chgalg.htmpl
- detail_chgcat.htmpl
- detail_chgstat.htmpl
- detail_chgtype.htmpl

- detail_CI_ACTIONS.htmpl
- detail_CI_ACTIONS_ALTERNATE.htmpl
- detail_CI_DOC_TEMPLATES.htmpl
- detail_CI_STATUSES.htmpl
- detail_CI_WF_TEMPLATES.htmpl
- detail_cmth.htmpl
- detail_cnote.htmpl
- detail_cnt.htmpl
- detail_cost_cntr.htmpl
- detail_country.htmpl
- detail_cr.htmpl
- detail_crs.htmpl
- detail_crsq.htmpl
- detail_cr_prptpl.htmpl
- detail_ctab.htmpl
- detail_ctimer.htmpl
- detail_ctp.htmpl
- detail_dcon.htmpl
- detail_dept.htmpl
- detail_dmn.htmpl
- detail_doc_rep.htmpl
- detail_DOC_VERSIONS.htmpl
- detail_EBR_ACRONYMS.htmpl
- detail_EBR_LOG.htmpl
- detail_EBR_NOISE_WORDS.htmpl
- detail_EBR_SYNONYMS_ADM.htmpl
- detail_event_log.htmpl
- detail_evt.htmpl
- detail_fmgrp.htmpl
- detail_grc.htmpl
- detail_g_cnt.htmpl
- detail_g_loc.htmpl
- detail_g_org.htmpl

- detail_g_prod.htmpl
- detail_g_qname.htmpl
- detail_g_srvrs.htmpl
- detail_g_tblmap.htmpl
- detail_g_tblrule.htmpl
- detail_help_set.htmpl
- detail_hier_edit.htmpl
- detail_hier_ro.htmpl
- detail_ical_event_template.htmpl
- detail_imp.htmpl
- detail_in.htmpl
- detail_iss.htmpl
- detail_issalg.htmpl
- detail_isscat.htmpl
- detail_issstat.htmpl
- detail_iss_wf.htmpl
- detail_kc.htmpl
- detail_KCAT.htmpl
- detail_KD.htmpl
- detail_KD_FILE.htmpl
- detail_KD_QA.htmpl
- detail_KD_SAVE_AS.htmpl
- detail_KD_TASK.htmpl
- detail_KD_TASK_cancel_rework.htmpl
- detail_KD_TASK_retire.htmpl
- detail_KD_template.htmpl
- detail_KEIT_TEMPLATES.htmpl
- detail_KT_ACT_CONTENT.htmpl
- detail_KT_BLC.htmpl
- detail_KT_FILE_TYPE.htmpl
- detail_KT_FLG_TYPE.htmpl
- detail_ldap.htmpl
- detail_ldap_group.htmpl

- detail_loc.htmpl
- detail_LONG_TEXTS.htmpl
- detail_lr_ro.htmpl
- detail_macro.htmpl
- detail_macro_type.htmpl
- detail_menu_bar.htmpl
- detail_menu_tree_name.htmpl
- detail_mfrmod.htmpl
- detail_mgs.htmpl
- detail_mgsalg.htmpl
- detail_mgsstat.htmpl
- detail_NOTIFICATION.htmpl
- detail_no_contract_sdsc.htmpl
- detail_nr.htmpl
- detail_nrf.htmpl
- detail_nr_com.htmpl
- detail_ntfl.htmpl
- detail_ntfm.htmpl
- detail_ntfr.htmpl
- detail_options.htmpl
- detail_org.htmpl
- detail_O_COMMENTS.htmpl
- detail_O_EVENTS.htmpl
- detail_pcat.htmpl
- detail_perscnt.htmpl
- detail_position.htmpl
- detail_pr.htmpl
- detail_prefs.htmpl
- detail_pri.htmpl
- detail_prod.htmpl
- detail_projex.htmpl
- detail_prptpl.htmpl
- detail_prpval.htmpl

- detail_prpval_rule.htmpl
- detail_prp_edit.htmpl
- detail_QUERY_POLICY.htmpl
- detail_rc.htmpl
- detail_response.htmpl
- detail_role.htmpl
- detail_role_go_form.htmpl
- detail_rptmeth.htmpl
- detail_rrf.htmpl
- detail_rss.htmpl
- detail_sapolicy.htmpl
- detail_saprobtyp.htmpl
- detail_sdsc.htmpl
- detail_sdsc_map.htmpl
- detail_seq.htmpl
- detail_sev.htmpl
- detail_site.htmpl
- detail_slatpl.htmpl
- detail_srvr_aliases.htmpl
- detail_srvr_zones.htmpl
- detail_state.htmpl
- detail_svc_contract.htmpl
- detail_svy_atpl.htmpl
- detail_svy_qtpl.htmpl
- detail_svy_tpl.htmpl
- detail_tab.htmpl
- detail_tenant.htmpl
- detail_tenant_group.htmpl
- detail_tskstat.htmpl
- detail_tskty.htmpl
- detail_tspan.htmpl
- detail_typecnt.htmpl
- detail_tz.htmpl

- detail_urg.htmpl
- detail_USP_PREFERENCES.htmpl
- detail_usp_servers.htmpl
- detail_vpt.htmpl
- detail_web_form.htmpl
- detail_wf.htmpl
- detail_wftpl.htmpl
- detail_wrkshft.htmpl
- dmn_dcon_tab.htmpl
- edit_prop_dyn.htmpl
- ed_image_pane.htmpl
- evt_action_info.htmpl
- evt_config_info.htmpl

G

- generic.htmpl
- get_comment.htmpl
- g_profile_browser.htmpl
- g_profile_browser2,htmpl
- g_profile_browser3,htmpl
- g_profile_browser_frameset.htmpl
- g_profile_jump.htmpl
- g_profile_scratchpad.htmpl

H

- hierload_admin_tree.htmpl
- hierload_KCAT.htmpl
- hiersel_admin_tree.htmpl
- hiersel_KCAT.htmpl
- hourglass.htmpl
- html_editor_create_change_order.htmpl
- html_editor_create_ticket.htmpl
- html_editor_frames.htmpl
- html_editor_insert_image.htmpl

- html_editor_insert_link.htmpl
- html_editor_insert_table.htmpl
- html_editor_tabs.htmpl
- html_editor_toolbar.htmpl

I

- insert_iss_wf.htmpl
- insert_wf.htmpl
- in_relreq_tab.htmpl
- isscat_auto_assignment_tab.htmpl
- isscat_prptpl_tab.htmpl
- isscat_wftpl_tab.htmpl
- issue_status_change.htmpl
- iss_accumulate.htmpl
- iss_close_all_child.htmpl
- iss_custfld_tab.htmpl
- iss_expedite.htmpl
- iss_lr.htmpl
- iss_reliss_tab.htmpl
- iss_resol_tab.htmpl

K

- kd_action_forward.htmpl
- kd_action_publish.htmpl
- kd_action_reject.htmpl
- kd_action_unpublish.htmpl
- kd_action_unretire.htmpl
- kd_attachments_tab.htmpl
- kd_attributes_tab.htmpl
- kd_categories_tab.htmpl
- kd_content_tab.htmpl
- kd_file_prop_tab.htmpl
- kd_permissions_tab.htmpl
- kd_qa_attributes_tab.htmpl

- kd_qa_content_tab.htmpl
- keit_tmpl_export_fields_tab.htmpl
- keit_tmpl_export_filter_tab.htmpl
- keit_tmpl_import_settings_tab.htmpl
- keit_tmpl_name_tab.htmpl
- kt_admin_attachments.htmpl
- kt_admin_automated_policies.htmpl
- kt_admin_document_settings.htmpl
- kt_admin_faq_options.htmpl
- kt_admin_general_settings.htmpl
- kt_admin_integration.htmpl
- kt_admin_knowledge.htmpl
- kt_admin_parse_settings.htmpl
- kt_admin_report_card.htmpl
- kt_admin_search_config_cr.htmpl
- kt_admin_search_config_iss.htmpl
- kt_admin_search_options.htmpl
- kt_admin_survey_settings.htmpl
- kt_admin_workflow_settings.htmpl
- kt_architect.htmpl
- kt_architect2,htmpl
- kt_architect3,htmpl
- kt_architect_delete_KCAT.htmpl
- kt_architect_delete_KD.htmpl
- kt_architect_frameset.htmpl
- kt_architect_init.htmpl
- kt_architect_javascript.htmpl
- kt_architect_KCATs.htmpl
- kt_architect_KCAT_path.htmpl
- kt_architect_KDs.htmpl
- kt_dtbuilder.htmpl
- kt_dtbuilder2,htmpl
- kt_dtbuilder3,htmpl

- kt_dtbuilder_frameset.htmpl
- kt_dtbuilder_node.htmpl
- kt_dtbuilder_prompt_window.htmpl
- kt_dtbuilder_save_dialog_window.htmpl
- kt_dtbuilder_save_tree_form.htmpl
- kt_dtbuilder_tree.htmpl
- kt_email_document.htmpl
- kt_faq_tree.htmpl
- kt_main.htmpl
- kt_main2,htmpl
- kt_main3,htmpl
- kt_main_role.htmpl
- kt_permissions.htmpl

L

- list.template
- list_acctyp.htmpl
- list_act_type_assoc.htmpl
- list_alg.htmpl
- list_all_fmgrp.htmpl
- list_all_lr.htmpl
- list_architect_KDs.htmpl
- list_architect_KDs_Pref.htmpl
- list_arcpur_hist.htmpl
- list_arcpur_rule.htmpl
- list_atev.htmpl
- list_atomic_cond.htmpl
- list_attmnt.htmpl
- list_attr_alias.htmpl
- list_aty.htmpl
- list_audlog.htmpl
- list_bmcls.htmpl
- list_bmhier.htmpl

- list_bmrep.htmpl
- list_bm_task.htmpl
- list_bool.htmpl
- list_ca_cmpny.htmpl
- list_ca_logical_asset.htmpl
- list_chg.htmpl
- list_chgalg.htmpl
- list_chgcat.htmpl
- list_chgsched.htmpl
- list_chgsched_config.htmpl
- list_chgstat.htmpl
- list_chgtype.htmpl
- list_CI_ACTIONS.htmpl
- list_CI_ACTIONS_ALTERNATE.htmpl
- list_CI_DOC_TEMPLATES.htmpl
- list_CI_STATUSES.htmpl
- list_CI_WF_TEMPLATES.htmpl
- list_cmth.htmpl
- list_cnote.htmpl
- list_cnt.htmpl
- list_cost_cntr.htmpl
- list_country.htmpl
- list_cr.htmpl
- list_crs.htmpl
- list_crsq.htmpl
- list_crs_cr.htmpl
- list_crs_in.htmpl
- list_crs_pr.htmpl
- list_crt.htmpl
- list_cr_kt.htmpl
- list_ctab.htmpl
- list_ctimer.htmpl
- list_ctp.htmpl

- list_dcon.htmpl
- list_dept.htmpl
- list_dmn.htmpl
- list_DOC_VERSIONS.htmpl
- list_EBR_ACRONYMS.htmpl
- list_EBR_LOG.htmpl
- list_EBR_NOISE_WORDS.htmpl
- list_EBR_SYNONYMS_ADM.htmpl
- list_event_log.htmpl
- list_evt.htmpl
- list_evtdly.htmpl
- list_grc.htmpl
- list_grpmem.htmpl
- list_g_chg_queue.htmpl
- list_g_cnt.htmpl
- list_g_cr_queue.htmpl
- list_g_iss_queue.htmpl
- list_g_loc.htmpl
- list_g_org.htmpl
- list_g_prod.htmpl
- list_g_qname.htmpl
- list_g_srvrs.htmpl
- list_g_tblmap.htmpl
- list_g_tblrule.htmpl
- list_g_tenant.htmpl
- list_help_item.htmpl
- list_help_set.htmpl
- list_ical_event_template.htmpl
- list_imp.htmpl
- list_in.htmpl
- list_iss.htmpl
- list_issalg.htmpl
- list_isscat.htmpl

- list_issstat.htmpl
- list_iss_kt.htmpl
- list_iss_wf.htmpl
- list_kc.htmpl
- list_KCAT_LINKED.htmpl
- list_KCAT_QA.htmpl
- list_KCAT_tree.htmpl
- list_KD.htmpl
- list_kdsched.htmpl
- list_kdsched_config.htmpl
- list_KD_ATTMNT.htmpl
- list_kd_CI_DOC_LINKS.htmpl
- list_KD_FILE.htmpl
- list_kd_INDEX_DOC_LINKS.htmpl
- list_KD_QA.htmpl
- list_KEIT_export_transactions.htmpl
- list_KEIT_IMPORT_PACKAGES.htmpl
- list_KEIT_import_transactions.htmpl
- list_KEIT_TEMPLATES.htmpl
- list_KT_ACT_CONTENT.htmpl
- list_KT_BLC.htmpl
- list_KT_FILE_TYPE.htmpl
- list_KT_FLG_TYPE.htmpl
- list_KT_FREE_TEXT.htmpl
- list_KT_LIFE_CYCLE_REP.htmpl
- list_ldap.htmpl
- list_ldap_group.htmpl
- list_loc.htmpl
- list_LONG_TEXTS.htmpl
- list_lr.htmpl
- list_macro.htmpl
- list_macro_type.htmpl
- list_menu_bar.htmpl

- list_menu_tree_name.htmpl
- list_mfrmod.htmpl
- list_mgs.htmpl
- list_mgsalg.htmpl
- list_mgsstat.htmpl
- list_NOTIFICATION.htmpl
- list_no_contract_sdsc.htmpl
- list_nr.htmpl
- list_nrf.htmpl
- list_nr_com.htmpl
- list_ntfl.htmpl
- list_ntfm.htmpl
- list_ntfr.htmpl
- list_OA_TABLES.htmpl
- list_options.htmpl
- list_org.htmpl
- list_O_EVENTS.htmpl
- list_pcat.htmpl
- list_pcat_cr.htmpl
- list_pcat_in.htmpl
- list_pcat_pr.htmpl
- list_perscnt.htmpl
- list_position.htmpl
- list_pr.htmpl
- list_pri.htmpl
- list_prod.htmpl
- list_prod_list.htmpl
- list_prpval.htmpl
- list_prpval_rule.htmpl
- list_QUERY_POLICY.htmpl
- list_QUERY_POLICY_ACTIONS.htmpl
- list_rc.htmpl
- list_rel_cat.htmpl

- list_response.htmpl
- list_role.htmpl
- list_role_tab.htmpl
- list_rptmeth.htmpl
- list_rrf.htmpl
- list_rss.htmpl
- list_sapolicy.htmpl
- list_saprobtyp.htmpl
- list_sdsc.htmpl
- list_sdsc_map.htmpl
- list_seq.htmpl
- list_sev.htmpl
- list_showgrp.htmpl
- list_site.htmpl
- list_srvr_aliases.htmpl
- list_srvr_zones.htmpl
- list_state.htmpl
- list_svc_contract.htmpl
- list_svy_atpl.htmpl
- list_svy_qtpl.htmpl
- list_svy_tpl.htmpl
- list_tab.htmpl
- list_tenant.htmpl
- list_tenant_group.htmpl
- list_tskstat.htmpl
- list_tskty.htmpl
- list_tspan.htmpl
- list_typecnt.htmpl
- list_tz.htmpl
- list_urg.htmpl
- list_usp_servers.htmpl
- list_vpt.htmpl
- list_web_form.htmpl

- list_wf.htmpl
- list_wrkshft.htmpl
- load_properties.htmpl
- load_wait.htmpl
- loc_address_tab.htmpl
- loc_auto_assignment_tab.htmpl
- log_reader.htmpl
- log_reader_banner.htmpl
- log_reader_fs.htmpl
- log_sol_4itil.htmpl

M

- macro_atomic_cond_tab.htmpl
- macro_cnt_tab.htmpl
- macro_ctp_tab.htmpl
- macro_ntfl_tab.htmpl
- macro_rrf_tab.htmpl
- mactyp_exescript_tab.htmpl
- mactyp_valscript_tab.htmpl
- mapped_contracts_tab.htmpl
- menubar.template
- menubar_admin.htmpl
- menubar_architect.htmpl
- menubar_chg_sched.htmpl
- menubar_dtbuilder.htmpl
- menubar_html_editor.htmpl
- menubar_kt.htmpl
- menubar_no.htmpl
- menubar_sd.htmpl
- menubar_sd_chg_manager.htmpl
- menubar_sd_cust_mgr.htmpl
- menubar_sd_cust_rep.htmpl
- menubar_sd_hd_manager.htmpl

- menubar_sd_inc_manager.htmpl
- menubar_sd_know_analyst.htmpl
- menubar_sd_know_manager.htmpl
- menubar_sd_l1_analyst.htmpl
- menubar_sd_l2_analyst.htmpl
- menubar_sd_prb_manager.htmpl
- menubar_sd_vendor_analyst.htmpl
- menu_frames.htmpl
- menu_tree_editor.htmpl
- menu_tree_editor2.htmpl
- menu_tree_editor3.htmpl
- mgs_cnt_tab.htmpl
- mgs_ctp_tab.htmpl
- mgs_ini_tab.htmpl
- mgs_ntfl_tab.htmpl
- mgs_rem_tab.htmpl
- multiframe.template
- multiframe_reports_admin.htmpl
- multiframe_reports_chg_manager.htmpl
- multiframe_reports_cust_mgr.htmpl
- multiframe_reports_inc_mgr.htmpl
- multiframe_reports_know_analyst.htmpl
- multiframe_reports_know_mgr.htmpl
- multiframe_reports_prb_mgr.htmpl
- multiframe_reports_sd_mgr.htmpl

N

- new_lr.htmpl
- nf.htmpl
- nosession.htmpl
- nr_bm_tab.htmpl
- nr_chg_tab.htmpl
- nr_contact_tab.htmpl

- nr_inc_tab.htmpl
- nr_inv_tab.htmpl
- nr_iss_tab.htmpl
- nr_loc_tab.htmpl
- nr_log_tab.htmpl
- nr_org_tab.htmpl
- nr_prb_tab.htmpl
- nr_projex_tab.htmpl
- nr_rel_tab.htmpl
- nr_reqitil_tab.htmpl
- nr_req_tab.htmpl
- nr_serv_tab.htmpl
- ntfl_ntfr_tab.htmpl
- ntfr_aty_tab.htmpl
- ntfr_cnt_tab.htmpl
- ntfr_ctp_tab.htmpl
- ntfr_ntfl_tab.htmpl

O

- order_status_change.htmpl
- org_address_tab.htmpl
- org_env_tab.htmpl

P

- pcat_auto_assignment_tab.htmpl
- pcat_prptpl_tab.htmpl
- pcat_wftpl_tab.htmpl
- power_user_tips.htmpl
- profile_browser.htmpl
- profile_browser2.htmpl
- profile_browser3.htmpl
- profile_browser_frameset.htmpl
- profile_envcnt.htmpl
- profile_envorg.htmpl

- profile_histcnt_chg.htmpl
- profile_histcnt_cr.htmpl
- profile_histcnt_in.htmpl
- profile_histcnt_iss.htmpl
- profile_histcnt_pr.htmpl
- profile_historg_chg.htmpl
- profile_historg_cr.htmpl
- profile_historg_in.htmpl
- profile_historg_iss.htmpl
- profile_historg_pr.htmpl
- profile_infocnt.htmpl
- profile_infoorg.htmpl
- profile_menu.htmpl
- profile_qtemplate.htmpl
- pr_attinc_tab.htmpl
- pr_relreq_tab.htmpl

R

- reports.htmpl
- reports.htmpl.tpl
- request_status_change.htmpl
- role_auth_tab.htmpl
- role_fnacc_tab.htmpl
- role_goform_tab.htmpl
- role_kt_ct_tab.htmpl
- role_kt_docs_tab.htmpl
- role_webform_tab.htmpl
- role_web_interface_tab.htmpl

S

- sapolicy_ac_tab.htmpl
- sapolicy_pt_tab.htmpl
- saprobtyp_dh_tab.htmpl
- saprobtyp_rd_tab.htmpl

- scoreboard.htmpl
- scratchpad.htmpl
- screen_reader_usage.htmpl
- sdsc_chg_slatpl_tab.htmpl
- sdsc_chg_wf_slatpl_tab.htmpl
- sdsc_cr_slatpl_tab.htmpl
- sdsc_iss_slatpl_tab.htmpl
- sdsc_iss_wf_slatpl_tab.htmpl
- sdsc_map_cnt_tab.htmpl
- sdsc_map_grp_tab.htmpl
- sdsc_map_nr_tab.htmpl
- sdsc_map_pri_tab.htmpl
- sdsc_map_urg_tab.htmpl
- sd_kt_admin.htmpl
- sd_main.htmpl
- sd_main_role.htmpl
- search_child_KCATs_filter.htmpl
- show_error.htmpl
- show_main_detail.htmpl
- std_body.htmpl
- std_body_site.htmpl
- std_footer.htmpl
- std_footer_site.htmpl
- std_head.htmpl
- std_head_site.htmpl
- suggest_knowledge_isscat.htmpl
- suggest_knowledge_list_isscat.htmpl
- suggest_knowledge_list_pcat.htmpl
- suggest_knowledge_pcat.htmpl
- sugggest_knowledge_search_options.htmpl

T

- tab_detail.template

- tenant_address_tab.htmpl
- tenant_groups_tab.htmpl
- tenant_group_members_tab.htmpl
- tskty_tskstat_tab.htmpl

U

- update_lrel_bmrep.htmpl
- update_lrel_chg.htmpl
- update_lrel_chgcat.htmpl
- update_lrel_cnt.htmpl
- update_lrel_cr.htmpl
- update_lrel_ctp.htmpl
- update_lrel_goform.htmpl
- update_lrel_help_content.htmpl
- update_lrel_in.htmpl
- update_lrel_iss.htmpl
- update_lrel_isscat.htmpl
- update_lrel_loc.htmpl
- update_lrel_macro.htmpl
- update_lrel_nr.htmpl
- update_lrel_ntfl.htmpl
- update_lrel_ntfr.htmpl
- update_lrel_org.htmpl
- update_lrel_pcat.htmpl
- update_lrel_pr.htmpl
- update_lrel_role.htmpl
- update_lrel_tab.htmpl
- update_lrel_tenant.htmpl
- update_lrel_tenant_group.htmpl
- update_lrel_tskstat.htmpl
- update_lrel_webform.htmpl
- update_lrel_wrkshft.htmpl
- upd_chg_sched.htmpl

- upload_file.html
- upload_success.htmpl
- usq_update.htmpl
- usq_update_control.htmpl
- usq_update_fin.htmpl
- usq_update_select.htmpl
- usq_update_tree.htmpl

V

- v30_date_helper.htmpl

W

- wfdef.htmpl
- wftpl_auto_assignment_tab.htmpl
- wftpl_bhvtpl_tab.htmpl
- working.htmpl
- workitems.htmpl
- wrkshft_auto_assignment_tab.htmpl
- wrkshft_schedule_tab.htmpl
- wspmain.htmpl

X

- xfer_esc_chg.htmpl
- xfer_esc_cr.htmpl
- xfer_esc_iss.htmpl
- xx_attmnt_tab.htmpl
- xx_candp_tab.htmpl
- xx_nr_tab.htmpl
- xx_prop_tab.htmpl
- xx_solnalg_tab.htmpl
- xx_stype_tab.htmpl
- xx_template_tab.htmpl
- xx_wf_tab.htmpl

Appendice D: Codici risultato LDAP - RFC 2251

Questa sezione contiene i seguenti argomenti:

Codici restituiti LDAP (a pagina 1249)
Codici di ritorno del server LDAP (a pagina 1249)
Codici di ritorno del client LDAP (a pagina 1255)
Standard RFC associati LDAP (a pagina 1257)

Codici restituiti LDAP

LDAP prevede una serie di codici relativi a risultati di operazioni che possono essere generati dal server LDAP in risposta a diverse richieste LDAP. Questi codici indicano lo stato dell'operazione di protocollo e sono classificati in base a categorie di codici di ritorno del server o del client.

Codici di ritorno del server LDAP

Nella tabella seguente vengono elencati i codici restituzione server:

Valore esadecimale	Valore decimale	Descrizione
0x00	0	LDAP_SUCCESS Indica che l'operazione richiesta dal client è stata completata correttamente.
0x01	1	LDAP_OPERATIONS_ERROR Indica che si è verificato un errore interno. Il server non è in grado di rispondere con un errore più specifico né di rispondere correttamente a una richiesta. Questo codice non indica che il client ha inviato un messaggio non valido.
0x02	2	LDAP_PROTOCOL_ERROR Indica che il server ha ricevuto una richiesta non valida dal client.
0x03	3	LDAP_TIMELIMIT_EXCEEDED Indica che è stato superato il tempo massimo disponibile per l'operazione specificato dal client o dal server. Nelle operazioni di ricerca, vengono restituiti risultati non completi.

Valore esadecimale	Valore decimale	Descrizione
0x04	4	LDAP_SIZELIMIT_EXCEEDED Indica che, in un'operazione di ricerca, è stato superato il tempo massimo disponibile specificato dal client o dal server. Vengono restituiti risultati non completi.
0x05	5	LDAP_COMPARE_FALSE Non indica una condizione di errore. Indica che un'operazione di confronto ha restituito un valore False.
0x06	6	LDAP_COMPARE_TRUE Non indica una condizione di errore. Indica che un'operazione di confronto ha restituito un valore True.
0x07	7	LDAP_AUTH_METHOD_NOT_SUPPORTED Indica che durante un'operazione di binding il client ha richiesto un metodo di autenticazione non supportato dal server LDAP.
0x08	8	LDAP_STRONG_AUTH_REQUIRED Indica una delle condizioni seguenti: ■ Nelle richieste di binding, il server LDAP accetta solo autenticazioni dettagliate. ■ In una richiesta client, il client ha richiesto un'operazione, ad esempio un'eliminazione, che richiede un'autenticazione dettagliata. ■ In una notifica di disconnessione non richiesta, il server LDAP ha rilevato che si è verificato un errore imprevisto nel sistema di sicurezza che protegge le comunicazioni tra il server e il client oppure che tale sistema è stato compromesso.
0x09	9	Operazione riservata.
0x0A	10	LDAP_REFERRAL Non indica una condizione di errore. In LDAPv3, indica che il server non contiene l'elemento di destinazione della richiesta, mentre i server nel campo di riferimento potrebbero contenerlo.
0x0B	11	LDAP_ADMINLIMIT_EXCEEDED Indica che è stato superato il limite del server LDAP impostato da un'autorità amministrativa.
0x0C	12	LDAP_UNAVAILABLE_CRITICAL_EXTENSION Indica che il server LDAP non è riuscito a soddisfare una richiesta poiché non erano disponibili una o più estensioni critiche. Il server non supporta il controllo oppure il controllo non è appropriato per il tipo di operazione.

Valore esadecimale	Valore decimale	Descrizione
0x0D	13	LDAP_CONFIDENTIALITY_REQUIRED Indica che la sessione non è protetta da un protocollo, quale il protocollo TLS (Transport Layer Security), che ne assicura la riservatezza.
0x0E	14	LDAP_SASL_BIND_IN_PROGRESS Non indica una condizione di errore, ma che il server è pronto per il successivo passaggio del processo. Per continuare il processo, il client deve inviare al server lo stesso meccanismo SASL.
0x0F	15	Non utilizzato.
0x10	16	LDAP_NO_SUCH_ATTRIBUTE Indica che l'attributo specificato nell'operazione di modifica o di confronto non esiste nell'elemento.
0x11	17	LDAP_UNDEFINED_TYPE Indica che l'attributo specificato nell'operazione di modifica o di aggiunta non esiste nello schema del server LDAP.
0x12	18	LDAP_INAPPROPRIATE_MATCHING Indica che la regola di corrispondenza specificata nel filtro di ricerca non corrisponde a una regola definita per la sintassi dell'attributo.
0x13	19	LDAP_CONSTRAINT_VIOLATION Indica che il valore dell'attributo specificato in un'operazione di modifica, aggiunta o modifica DN viola i vincoli impostati sull'attributo. Il vincolo può fare riferimento alle dimensioni o al contenuto (solo stringa, no binario).
0x14	20	LDAP_TYPE_OR_VALUE_EXISTS Indica che il valore dell'attributo specificato in un'operazione di modifica o aggiunta esiste già come valore per l'attributo.
0x15	21	LDAP_INVALID_SYNTAX Indica che il valore dell'attributo specificato in un'operazione di aggiunta, confronto o modifica non è riconosciuto oppure la sintassi non è valida per l'attributo.
	22-31	Non utilizzato.
0x20	32	LDAP_NO_SUCH_OBJECT Indica che non è possibile trovare l'oggetto di destinazione. Questo codice non viene restituito nelle operazioni seguenti: ■ Operazioni di ricerca che trovano la base di ricerca, ma non trovano voci che corrispondono al filtro di ricerca. ■ Operazioni di binding.

Valore esadecimale	Valore decimale	Descrizione
0x21	33	LDAP_ALIAS_PROBLEM Indica che si è verificato un errore quando è stato annullato il riferimento di un alias.
0x22	34	LDAP_INVALID_DN_SYNTAX Indica che la sintassi del DN non è valida. Tuttavia, se la sintassi del DN è corretta, ma le regole della struttura del server LDAP non consentono l'operazione, il server restituisce il codice seguente: LDAP_UNWILLING_TO_PERFORM
0x23	35	LDAP_IS_LEAF Indica che l'operazione specificata non può essere eseguita su un elemento di tipo foglia. Questo codice non è attualmente presente nelle specifiche LDAP, ma è riservato per questa costante.
0x24	36	LDAP_ALIAS_DEREF_PROBLEM Indica che durante un'operazione di ricerca, il client non dispone dei diritti di accesso per leggere il nome dell'oggetto con alias oppure che l'operazione di annullamento dell'alias non è consentita.
	37-47	Non utilizzato.
0x30	48	LDAP_INAPPROPRIATE_AUTH Indica che durante un'operazione di binding, il client sta tentando di utilizzare in modo non corretto un metodo di autenticazione. Ad esempio, la causa dell'errore potrebbe essere una delle seguenti: ■ Il client restituisce credenziali semplici quando invece sono richieste credenziali dettagliate. ■ Il client restituisce un DN e una password per un binding semplice ma nell'elemento non è definita la password.
0x31	49	LDAP_INVALID_CREDENTIALS Indica che durante un'operazione di binding, si è verificata una delle condizioni seguenti: ■ Il client ha passato una password o un DN non valido. ■ La password non è valida perché è scaduta, il programma di rilevamento delle intrusioni ha bloccato l'account oppure altri motivi simili.
0x32	50	LDAP_INSUFFICIENT_ACCESS Indica che il chiamante non dispone delle autorizzazioni sufficienti per eseguire l'operazione richiesta.

Valore esadecimale	Valore decimale	Descrizione
0x33	51	LDAP_BUSY Indica che il server LDAP è troppo occupato per elaborare subito la richiesta del client. Se il client attende e quindi invia nuovamente la richiesta, il server potrebbe essere in grado di elaborarla.
0x34	52	LDAP_UNAVAILABLE Indica che il server LDAP non è in grado di elaborare la richiesta di binding del client. Solitamente, questo codice indica che il server è in fase di arresto.
0x35	53	LDAP_UNWILLING_TO_PERFORM Indica che il server LDAP non è in grado di elaborare la richiesta a causa delle restrizioni definite dal server. Questo errore viene restituito per i motivi seguenti: ■ La richiesta dell'elemento di aggiunta viola le regole di struttura del server. ■ La richiesta dell'attributo di modifica specifica attributi che l'utente non può modificare. ■ Le restrizioni applicate alla password impediscono l'azione. ■ Le restrizioni applicate alla connessione impediscono l'azione.
0x36	54	LDAP_LOOP_DETECT Indica che il client ha rilevato un alias oppure un loop del riferimento e non è in grado di completare la richiesta.
	55-63	Non utilizzato.
0x40	64	LDAP_NAMING_VIOLATION Indica che l'operazione di aggiunta o modifica DN viola le regole di struttura dello schema. Ad esempio: ■ La richiesta inserisce il subordinato di un elemento in un alias. ■ La richiesta inserisce il subordinato di un elemento in un contenitore non consentito a causa delle regole di contenimento. ■ Il nome RDN relativo all'elemento utilizza un tipo di attributo non consentito.

Valore esadecimale	Valore decimale	Descrizione
0x41	65	LDAP_OBJECT_CLASS_VIOLATION Indica che l'operazione di aggiunta, modifica o modifica DN viola le regole della classe oggetto relative all'elemento. Ad esempio, l'errore è restituito dai seguenti tipi di richiesta: ■ L'operazione di aggiunta o modifica tenta di aggiungere un elemento senza un valore per un attributo richiesto. ■ L'operazione di aggiunta o modifica tenta di aggiungere un elemento con un valore per un attributo che non è presente nella definizione della classe. ■ L'operazione di modifica tenta di rimuovere un attributo richiesto senza eliminare la classe ausiliaria che definisce l'attributo, come previsto.
0x42	66	LDAP_NOT_ALLOWED_ON_NONLEAF Indica che l'operazione richiesta è consentita solo per gli elementi di tipo foglia. Ad esempio, l'errore viene restituito dai seguenti tipi di richiesta: ■ Il client ha richiesto un'operazione di eliminazione per un elemento di tipo padre. ■ Il client ha richiesto un'operazione di modifica DN per un elemento di tipo padre.
0x43	67	LDAP_NOT_ALLOWED_ON_RDN Indica che l'operazione di modifica ha tentato di eliminare un valore di attributo che forma il DN dell'elemento.
0x44	68	LDAP_ALREADY_EXISTS Indica che l'operazione di aggiunta ha tentato di aggiungere un elemento che esiste già oppure che l'operazione di modifica ha tentato di rinominare un elemento con il nome di un elemento che esiste già.
0x45	69	LDAP_NO_OBJECT_CLASS_MODS Indica che l'operazione di modifica ha tentato di modificare le regole della struttura di una classe oggetto.
0x46	70	LDAP_RESULTS_TOO_LARGE Riservato per CLDAP.
0x47	71	LDAP_AFFECTS_MULTIPLE_DSAS Indica che l'operazione di modifica DN riguarda lo spostamento di un elemento da un server LDAP a un altro e pertanto richiede più di un server LDAP.
	72-79	Non utilizzato.

Valore esadecimale	Valore decimale	Descrizione
0x50	80	LDAP_OTHER Indica una condizione di errore sconosciuta. È il valore predefinito dei codici di errore NDS che non hanno corrispondenza con altri codici di errore LDAP.

Codici di ritorno del client LDAP

Nella tabella seguente vengono elencati i codici restituzione client:

Valore esadecimale	Valore decimale	Descrizione
0x51	81	LDAP_SERVER_DOWN Indica che le librerie LDAP non sono in grado di stabilire una connessione iniziale con il server LDAP. Il server LDAP non è attivo oppure il nome host o il numero di porta specificati non sono validi.
0x52	82	LDAP_LOCAL_ERROR Indica che si è verificato un errore nel client LDAP. Solitamente, si tratta di un errore di allocazione della memoria dinamica.
0x53	83	LDAP_ENCODING_ERROR Indica che si sono verificati errori nel client LDAP durante la codifica di una richiesta LDAP destinata al server LDAP.
0x54	84	LDAP_DECODING_ERROR Indica che si sono verificati errori nel client LDAP durante la codifica di una risposta LDAP inviata dal server LDAP.
0x55	85	LDAP_TIMEOUT Indica che il client LDAP ha superato il tempo limite massimo durante l'attesa dei risultati.
0x56	86	LDAP_AUTH_UNKNOWN Indica che le funzioni ldap_bind o ldap_bind_s sono state richiamate con un metodo di autenticazione sconosciuto.
0x57	87	LDAP_FILTER_ERROR Indica che la funzione ldap_search è stata richiamata con un filtro di ricerca non valido.
0x58	88	LDAP_USER_CANCELLED Indica che l'utente ha annullato l'operazione LDAP.

Valore esadecimale	Valore decimale	Descrizione
0x59	89	LDAP_PARAM_ERROR Indica che una funzione LDAP è stata richiamata con un parametro non valido (ad esempio, il parametro ID è NULL).
0x5A	90	LDAP_NO_MEMORY: Indica che una funzione di allocazione della memoria dinamica non è riuscita durante la chiamata a una funzione LDAP.
0B	91	LDAP_CONNECT_ERROR Indica che il client LDAP ha perso la connessione oppure non è in grado di stabilire una connessione con il server LDAP.
0x5C	92	LDAP_NOT_SUPPORTED Indica che il client non supporta la funzionalità richiesta. Ad esempio, se il client LDAP è definito come client LDAPv2, le librerie impostano questo codice di errore quando il client richiede la funzionalità LDAPv3.
0x5D	93	LDAP_CONTROL_NOT_FOUND Indica che il client ha richiesto un controllo che le librerie non riescono a trovare nell'elenco dei controlli supportati inviato dal server LDAP.
0x5E	94	LDAP_NO_RESULTS_RETURNED Indica che il server LDAP non ha inviato risultati. Quando viene richiamata la funzione ldap_parse_result, nella risposta del server non viene incluso alcun codice risultato.
0x5F	95	LDAP_MORE_RESULTS_TO_RETURN Indica che il messaggio dei risultati include più risultati. Le librerie impostano questo codice quando con la chiamata alla funzione ldap_parse_result vengono rilevati altri codici risultato disponibili.
0x60	96	LDAP_CLIENT_LOOP Indica che le librerie LDAP hanno rilevato un loop. Solitamente, questo errore si verifica quando seguono dei riferimenti.
0x61	97	LDAP_REFERRAL_LIMIT_EXCEEDED Indica che il limite di hop del riferimento è stato superato. Il limite di hop determina quanti server può attraversare il client per recuperare i dati. Ad esempio, date le condizioni seguenti: ■ Il limite di hop è due. ■ Il riferimento è il server D che può essere contattato solo tramite il server B (1 hop) che contatta il server C (2 hop) che contatta il server D (3 hop) Con queste condizioni, il limite di hop viene superato e le librerie LDAP impostano questo codice.

Standard RFC associati LDAP

La tabella seguente descrive gli standard RFC associati a LDAP e disponibili per l'uso:

RFC	Descrizione
1274	Schema X.500 COSINE e Internet
1275	Requisiti di replica per fornire una directory Internet mediante X.500
1276	Estensioni per replica e operazioni distribuite per fornire una directory Internet mediante X.500
1308	Introduzione ai servizi di directory mediante il protocollo X.500
1309	Panoramica tecnica dei servizi di directory mediante il protocollo X.500
1430	Piano strategico per la distribuzione di un servizio di directory Internet X.500
1488	Rappresentazione di stringhe X.500 delle sintassi di attributi standard
1558	Rappresentazione di stringhe dei filtri di ricerca LDAP
1617	Linee guida per la denominazione e la struttura dei sistemi pilot delle directory X.500
1777	Protocollo LDAP v2
1778	Rappresentazione di stringhe delle sintassi di attributi standard
1779	Rappresentazione di stringhe dei nomi distinti
1804	Pubblicazione di schemi nella directory X.500
1823	Interfaccia dell'applicazione LDAP
1959	Formato URL LDAP
1960	Rappresentazione di stringhe dei filtri di ricerca LDAP
2044	UTF –8 - Formato di trasformazione di Unicode e ISO 10646
2164	Uso di una directory X.500/LDAP per il supporto del mapping degli indirizzi MIXER
2218	Schema comune per il servizio di pagine bianche di Internet
2247	Uso dei domini nei nomi distinti LDAP/X.500
2251	Protocollo LDAP (v3)
2252	LDAP (Lightweight Directory Access Protocol) (v3): definizioni della sintassi di attributo
2253	LDAP (Lightweight Directory Access Protocol) (v3): rappresentazione delle stringhe UTF-8 dei nomi distinti
2254	Rappresentazione di stringhe dei filtri di ricerca LDAP
2255	Formato URL LDAP
2256	Riepilogo dello schema utente X.500(96) per l'uso con LDAPv3

RFC	Descrizione
2279	UTF-8 – Formato di trasformazione di ISO 10646
2293	Rappresentazione di tabelle e strutture secondarie nella directory X.500
2294	Rappresentazione della gerarchia di indirizzi O/R nella struttura di informazioni della directory X.500
2307	Approccio all'uso di LDAP come servizio di informazioni sulla rete
2377	Piano di denominazione per applicazioni Internet directory-enabled
2531	Schema di funzioni per il contenuto per Internet Fax
2559	Protocolli operativi per infrastrutture di chiavi pubbliche Internet X.509 - LDAPv2
2587	Schema LDAPv2 per infrastrutture di chiavi pubbliche Internet X.509
2589	LDAP (Lightweight Directory Access Protocol) (v3): estensioni per servizi directory dinamici
2596	Uso dei codici lingua in LDAP
2649	Controllo LDAP e schema per la memorizzazione di firme delle operazioni
2657	RFC 2657 – Client LDAPv2 e struttura dell'indice
2696	Estensione del controllo LDAP per la gestione dei risultati a pagina semplice
2713	Schema per la rappresentazione degli oggetti Java(tm) in una directory LDAP
2714	Schema per la rappresentazione dei riferimenti agli oggetti CORBA in una directory LDAP
2739	Attributes di calendario per vCard e LDAP
2798	Definizione della classe di oggetti LDAP inetOrgPerson
2820	Requisiti di controllo dell'accesso per LDAP
2829	Metodi di autenticazione per LDAP
2830	LDAP (Lightweight Directory Access Protocol) (v3): estensione per la sicurezza dei livelli di trasporto
2849	Formato di interscambio dei dati LDAP (LDIF) - Specifiche tecniche
2879	Schema di funzioni per il contenuto per Internet Fax (V2)
2891	Estensione del controllo LDAP per l'ordinamento lato server dei risultati di ricerca
3045	Memorizzazione delle informazioni sui fornitori nella root DSE LDAP
3062	Operazione estesa di modifica della password LDAP
3112	Schema delle password di autenticazione LDAP
3296	Riferimenti subordinati denominati nelle directory del protocollo LDAP
3377	LDAP (Lightweight Directory Access Protocol) (v3): specifiche tecniche
3384	Requisiti di replica del protocollo LDAP (versione 3)